Japan. J. Math. 1, 25–85 (2006)
DOI: 10.1007/s11537-006-0502-5

JAPANESE JOURNAL OF MATHEMATICS
SINCE 1924

Travaux de Claude Chevalley sur la théorie du corps de classes: Introduction*

Shokichi Iyanaga

Received: 13 July 2005 / Accepted: 8 February 2006
Published online: 2 April 2006

Communicated by: Toshiyuki Kobayashi

Abstract. This article explains the contributions of Claude Chevalley to class field theory. His leading motivation on the subject seemed to be to give an "arithmetic proof" to the theory and to reveal the nature of the outstanding harmony of the Takagi–Artin class field theory, which had been established just at the time he started his research. His main achievements on the subject may have been the first arithmetic proof of the local class field theory without depending on the global theory, arithmetization of the global class field theory, and its generalization and presentation for infinite extensions by introducing ideles, which are now a kind of natural language in algebraic number theory. On the one hand, in this article we have attempted to provide rigorous mathematical description. On the other hand, although we have not demonstrated any proof, we have endeavored to show the development of the series of mathematical ideas that produced a variety of important concepts, bore fruit as class field theory, and then moved Chevalley to create his remarkable and influential works.

Keywords and phrases: class field theory, idele, C. Chevalley

Mathematics Subject Classification (2000): 11R37, 11-03, 01A61

* *Note by the Communicating Editor:* In the summer of 1994, the author began writing this article, having been invited to contribute it as an introduction to the *Collected Works of Claude Chevalley*, Volume 1. The author finished the work by the spring of 2000 and was waiting for its publication, but for reasons unrelated to the article, publication of the Chevalley volume was cancelled in 2005. Informed of the cancellation, Professor Iyanaga then chose to submit the article to this journal, the *Japanese Journal of Mathematics*, on July 13, 2005. (Toshiyuki Kobayashi on behalf of the author, who has been in hospital since the autumn of 2005.)

S. IYANAGA
Emeritus Professor, University of Tokyo, and member of the Japan Academy of Sciences

Dès l'époque où il étudiait à l'Ecole Normale Supérieure en 1926–29, Claude Chevalley s'est intéressé à la théorie des nombres et en particulier à la théorie du corps de classes, probablement sous l'influence de ses deux amis: Jacques Herbrand et André Weil, aînés de Chevalley d'un an et de trois ans, respectivement. Parmi les premiers travaux mathématiques publiés par Chevalley figure sa note (Herbrand [2]) en collaboration avec Herbrand: "Une nouvelle démonstration du théorème d'existence de la théorie du corps de classes" (1931). Herbrand avait publié déjà en 1930 sa note sur les unités d'un corps de nombres algébriques [1] et achevé sa thèse sur la théorie de la démonstration [3]. Il était un des meilleurs amis de Chevalley, et on s'était attendu à ce qu'il ait le plus brillant avenir comme mathématicien, mais il trouva malheureusement une mort tragique à 23 ans dans un accident de montagne en 1931, laissant d'inoubliables souvenirs à Chevalley. Weil avait commencé déjà à publier ses travaux arithmétiques dès 1927 (Weil [1]), et la collaboration Weil–Chevalley continue jusqu'à la fin de leur carrière (*cf.* Weil [3], [4], [5], [10], [12], Chevalley [7]). On peut bien imaginer l'enthousiasme de ces trois mathématiciens quand ils étudiaient ensemble à l'Ecole Normale Supérieure dans les années 1920 et apprirent les résultats encore récents de la théorie du corps de classes.

Je crois que cette théorie s'est placée au centre de l'intérêt de Chevalley dans son étude mathématique dans la première partie de sa carrière. Il en a donné trois exposés fondamentaux: d'abord dans sa Thèse [2] de 1932, où il a introduit les notions du groupe de Takagi et du groupe d'Artin, puis dans son mémoire [6] de 1940 dans les Annals, où il a donné la belle formulation avec la démonstration purement arithmétique de cette théorie au moyen de la notion d'idèles, introduite par lui dans son article [5] de 1936 dans le Journal de Liouville, et enfin dans son cours [8] de 1953 à l'Université de Nagoya utilisant la théorie cohomologique. Le but de mon Introduction[1] est d'expliquer le contenu des deux premiers [2], [6] de ces travaux avec les circonstances dans lesquelles ils ont été faits et leur signification historique dans le cours de l'évolution de l'arithmétique contemporaine. En ce qui concerne le troisième exposé [8], M. John Tate voudra bien en expliquer le contenu ainsi que le développement de cette théorie depuis les années 1950.

*

Dans les année 1920, où Chevalley commença à s'intéresser à cette théorie, la théorie arithmétique moderne n'était pas bien connue en France. En fait, elle s'était développée surtout en Allemagne depuis le début du 19^{e} siècle sous les influences des Disquisitiones Arithmeticae (Gauss [1]) où Gauss a ouvert une nouvelle voie en établissant des méthodes rigoureuses et systématiques: congruences, loi de réciprocité quadratique, formes quadratiques, cyclotomie. Gauss

[1] see ⋆.

[2] a introduit d'autre part les entiers complexes $a+bi$, $a,b \in \boldsymbol{Z}$ en étudiant la loi de réciprocité biquadratique. C'était le premier exemple d'*entiers algébriques* utilisés plus tard par Kummer dans ses recherches sur le problème de Fermat (Kummer [1]). Kummer a écrit l'équation de Fermat

$$x^p + y^p = z^p$$

sous la forme

$$x^p = (z-y)(z-\zeta_p y)\cdots(z-\zeta_p^{p-1}y)$$

où $\zeta_p = \exp(2\pi i/p)$ est une p-ième racine primitive de l'unité, p étant un nombre premier impair. L'ensemble des nombres

$$a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}, \quad a_0, a_1, \ldots, a_{p-1} \in \boldsymbol{Q}$$

forme le corps $\boldsymbol{Q}(\zeta_p)$ de *nombres cyclotomiques*, dont les nombres avec $a_i \in \boldsymbol{Z}$ forment l'*anneau des entiers cyclotomiques* que nous noterons A_p provisoirement. Si ces entiers se représentaient d'une manière unique comme produit d'"entiers premiers" comme dans l'anneau $\boldsymbol{Z}$ des entiers rationnels, il serait facile de démontrer la conjecture de Fermat. Mais il n'en est pas ainsi parce que d'abord l'anneau A_p des entiers cyclotomiques contient des *unités*, c'est-à-dire des éléments inversibles, beaucoup plus nombreux que $\boldsymbol{Z}$ ($\boldsymbol{Z}$ ne contient que deux unités ± 1 tandis que A_3 en contient 6 et A_p, $p > 3$ en contiennent une infinité), et même si l'on identifiait deux nombres $\alpha, \beta \in A_p$ quand α/β est une unité, la décomposablitié unique des entiers de A_p en "éléments premiers" n'est pas valable pour $p = 23$ par exemple. Kummer a introduit ce qu'il a nommé les "nombres idéaux" pour contourner cette difficulté et a pu démontrer la conjecture de Fermat pour une certaine catégorie de nombres premiers p dits "réguliers", sur laquelle nous reviendrons toute à l'heure.

*

La *théorie algébrique des nombres* commença ainsi par les travaux de Kummer sur le problème de Fermat. Elle fut présentée par Dedekind dans une forme bien organisée dans [3], dont il convient de rendre ici brièvement compte, parce que la théorie du corps de classes en est un chapitre. (Je suppose connus par le lecteur les concepts d'algèbre moderne, la théorie de Galois y comprise. On trouvera d'ailleurs les résultats qui vont suivre exposés avec démonstrations dans les premiers deux chapitres de Hilbert [2] ou dans les ouvrages comme Hecke [4], Samuel [1], Lang [1], [2] ou Takagi [7].)

Soit ξ une racine d'une équation irréductible de degré n à coefficients entiers

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0, \quad a_0, a_1, \ldots, a_n \in \boldsymbol{Z}.$$

L'ensemble des nombres de la forme

$$r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1}, \quad r_0, r_1 \ldots, r_{n-1} \in \boldsymbol{Q}$$

forme un *corps de nombres algébriques* $\boldsymbol{Q}(\xi)$ *de degré n* qui constitue un espace vectoriel de dimensions *n* sur $\boldsymbol{Q}$. (Chevalley considèrera plus tard vers la fin des 1930, aussi les extensions algébriques de degrés infinis de $\boldsymbol{Q}$. Cf. supra p.64. Mais dans la première partie de cette Introduction, nous entenderons toujours par les corps de nombres algébriques ceux de degrés finis.) Nous désignerons ce corps $\boldsymbol{Q}(\xi)$ par *k*. Tout élément de ce corps *k* satisfait à une équation algébrique irreductible de degré $\leq n$ à coefficents entiers. Ceux de ces éléments, pour lesquels le coefficients dominant (le coefficient du terme avec le plus haut degré) de l'équation est 1, forment un anneau A_k contenu dans *k*. Les éléments de A_k s'appellent les *entiers* de *k*. (Si $k = \boldsymbol{Q}$, on a $A_k = \boldsymbol{Z}$ et si $k = \boldsymbol{Q}(\zeta_p)$ on voit que A_k coincide avec ce que nous avons noté A_p.) Les éléments inversibles de A_k forment un groupe multiplicatif E_k, groupe des *unités* de A_k. Dirichlet [2] a démontré que E_k est produit direct d'un groupe cyclique fini, qui est le groupe des racines de l'unité contenues dans *k*, et d'un groupe abélien libre à $r_1 + r_2 - 1$ générateurs, où $r_1, 2r_2$ sont les nombres des corps conjugués réels et complexes de *k*.

Dedekind a remarqué que les "nombres idéaux" introduits par Kummer pour étudier l'arithmétique de $\boldsymbol{Q}(\zeta_p)$ peuvent se définir aussi dans un corps de nombres algébriques quelconque *k* et se représentent comme les "idéaux" (dans le sens habituel) de l'anneau A_k: un idéal *I* de A_k est un sousgroupe additif de A_k tel que pour tout $\alpha \in A_k$, on ait $\alpha I \subset I$. Pour les idéaux I, J, on peut définir le produit IJ comme le sousgroupe additif de A_k engendré par les produits $\alpha\beta$, $\alpha \in I, \beta \in J$, et on peut démontrer la décomposabilité unique des idéaux (non-nuls) de A_k en produit d'idéaux premiers. (Un ideal *P* s'appelle *premier* si $\alpha\beta \in P$ entraîne $\alpha \in P$ ou $\beta \in P$.) Aujourd'hui on exprime ce fait communément en disant que l'anneau A_k des entiers d'un corps de nombres algébriques *k* forme un *anneau de Dedekind*.

On introduit dans *k* en dehors des idéaux des A_k les idéaux dits fractionnaires. Un sousgroupe additif *I* de *k* s'appelle un *idéal fractionnaire* de *k* si, pour un certain $\alpha \in A_k, (\alpha \neq 0)$, αI devient un idéal de A_k. Les idéaux de A_k, qui sont naturellement aussi des idéaux fractionnaires, s'appelleront pour distinguer les *idéaux entiers*. La multiplication des idéaux entiers s'étend naturellement aux idéaux fractionnaires, pour laquelle ceux qui sont non nuls forment un groupe multiplicatif, abélien et libre, à une infinité de générateurs, qui sont les idéaux premiers de A_k. Nous désignerons ce groupe par F_k.

Dans les considérations multiplicatives, il est souvent commode d'exclure les l'élément inversibles, ce que nous indiquerons par le signe $\times$; par exemple $k^\times = k - \{0\}$; $k^\times$ forme un groupe multiplicatif, et si l'on note $(\alpha) = \alpha A_k$ pour $\alpha \in k^\times$, (α) est considéré comme un élément de F_k. Il s'appelle un *idéal principal* engendré par α. Si $\varepsilon \in E_k$, on a $(\varepsilon) = (1)$ et ceci est l'élément neutre du groupe F_k. L'ensemble des idéaux principaux $\{(\alpha); \alpha \in k^\times\}$ forme un sousgroupe de F_k, noté P_k, qui s'avère être un sousgroupe d'indice fini de F_k.

Le groupe quotient F_k/P_k s'appelle le *groupe des classes d'idéaux* de k, noté C_k, chaque élément de F_k/P_k est une *classe d'idéaux* et l'ordre de F_k/P_k est le *nombre des classes* de k; ce dernier se note h_k.

En revenant aux travaux de Kummer, celui-ci avait développé l'arithmétique de $k = \boldsymbol{Q}(\zeta_p)$ et a pu confirmer la conjecture de Fermat pour le cas où h_k n'est pas divisible par p. C'étaient ces nombres premiers p qu'il a appelé *réguliers*. Le groupe des classes d'idéaux de k mesure ainsi en un certain sens la difficulté de l'arithmétique de k.

*

Soit maintenant K une extension algébrique de degré fini de k. K est alors un autre corps de nombres algébriques, avec l'anneau des entiers A_K, le groupe des unités E_K, celui des idéaux F_K, celui des classes d'idéaux C_K etc. Comme $k \subset K$, on a évidemment $A_k \subset A_K$, $E_k \subset E_K$. Soit I un idéal entier de F_k, c'est-à-dire un idéal de A_k. I est un sous-ensemble de A_K et engendre un idéal I' de A_K que nous appellerons l'idéal de A_K (ou bien de K) *transféré* de I. On a évidemment $I \subset I'$, $I' \cap k = I$, et si J est un autre idéal de A_k, on a $(IJ)' = I'J'$. Il est facile de voir qu'à chaque idéal fractionnaire I de k correspond un idéal fractionnaire I' de K transféré de I de k, et quand I parcourt F_k, l'ensemble de I' forme un sousgroupe F_k' de F_K qui est isomorphe à F_k. Dorénavant nous identifierons I avec I' et F_k avec ce sousgroupe F_k' de F_K et écrirons $F_k \subset F_K$.

On a inventé l'arithmétique du corps de nombres algébriques pour traiter des problèmes concernant $\boldsymbol{Z}$ ou $\boldsymbol{Q}$. Ainsi un des problèmes fondamentaux de notre arithmétique est de savoir comment les idéaux premiers de k se comportent dans K. Soit P un idéal premier de A_k. Désignons toujours par P l'idéal de A_K tranféré de P. Il ne reste pas toujours premier dans K. (Par exemple le nombre premier 5 dans $\boldsymbol{Q}$ se factorise $5 = (2+i)(2-i)$ dans $\boldsymbol{Q}(i)$.) Soit

$$P = \overline{P}_1^{e_1} \cdots \overline{P}_g^{e_g}$$

la factorisation de P dans A_K (que nous appellerons aussi pour simplifier "la factorisation de P dans K"), $P_i, i = 1,2,\ldots,g$ étant des facteurs premiers de P dans K. Si $e_i \geq 2$ pour un $i \in \{1,2,\ldots,g\}$, on dit que P *se ramifie* dans K. On sait qu'il n'y a qu'un nombre fini d'idéaux premiers de k qui se ramifient dans K; ce sont seuls ceux qui divisent un certain idéal $D(K/k)$ de k qu'on appelle le *discriminant* de l'extension K/k. Si $D(K/k) = 1$, aucun idéal premier de k ne se ramifie dans K. On dit alors que l'extension K/k est *non-ramifiée*; autrement K/k est *ramifiée*. (Quand $k = \boldsymbol{Q}$, Minkowski a montré que toute extension $K(\neq k)$ est ramifiée.)

*

Si le degré $[K:k]$ de l'extension K/k est n, K a n corps conjugués $\sigma^{(i)}K = K^{(i)}, i = 1,2,\ldots,n$ sur k, $\sigma^{(i)}$ désignant les isomorphismes. (On peut supposer

$\sigma^{(1)} =$ identité, $K^{(1)} = K$.) On peut toujours construire l'extension galoisienne $\bar{K}/k$ contenant $K^{(i)}/k, i = 1,2,\ldots,n$. A tout idéal $\bar{I} = \bar{I}^{(1)}$ de $K = K^{(1)}$, correspond un idéal $\bar{I}^{(i)}$ de $K^{(i)} = \sigma^{(i)}K$ qui peut se transférer à un idéal $\bar{I}^{(i)}$ de $\bar{K}$. Le produit de ces idéaux $\prod_{i=1}^{n} \bar{I}^{(i)}$ est un idéal de $\bar{K}$ qui reste invariant par $\sigma^{(i)}, i = 1,\ldots,n$, et qui se représente comme un idéal de k. On appelle cet idéal de k la *norme* de l'idéal $\bar{I}$ dans l'extension K dans le corps de base k, et le désigne par $N_{K/k}(\bar{I})$. La formation $N_{K/k}$ de la norme de K/k est évidemment un homomorphisme du groupe F_K dans le groupe F_k. Et si k' est un corps intermédiaire entre k et $K : k \subset k' \subset K$, il est clair qu'on a $N_{k'/k} \cdot N_{K/k'} = N_{K/k}$.

Si $\bar{P}$ est un idéal premier de K, on montre que $N_{K/k}(\bar{P})$ est une puissance P^f d'un idéal premier P de k, et on appelle f le *degré* (relatif) de $\bar{P}$ par rapport à k. (En particulier, la norme $N_{k/\boldsymbol{Q}}(P)$ d'un idéal premier P de k au $\boldsymbol{Q}$ est une puissance p^{f_0} d'un nombre premier p. f_0 s'appelle la *norme absolue* de P. On montre aussi $P \cap \boldsymbol{Z} = (p)$ et que l'anneau quotient A_k/P est un corps fini à p^{f_0} éléments qui est l'extension du degré f_0 du corps fini $\boldsymbol{Z}/(p) \cong \boldsymbol{F}_p$ à p éléments.)

En formant les normes de K à k des deux membres de $P = \bar{P}_1^{e_1} \cdots \bar{P}_g^{e_g}$, on obtient $n = e_1 f_1 + \cdots + e_g f_g$ où f_i est le degré de $\bar{P}_i$ par rapport à k. On dit que P *se décompose complètement* dans K, si $e_1 = \cdots = e_g = f_1 = \cdots = f_g = 1$, $n = g$; et que P est *inerte* dans K si $e_1 = g = 1$, $f_1 = n$. En particulier, si K/k est galoisien, on a $f_1 = \cdots = f_g = f$, $e_1 = \cdots = e_g = e$, $n = efg$, et si P n'est pas ramifié, il suffit de savoir le degré f pour connaître le type de décomposition de P, K/k étant supposé donné.

*

Hilbert a écrit un rapport célèbre sur la théorie des corps de nombres algébriques [2] en 1897, nommé communément *Zahlbericht*, en réponse à la demande de la Société Mathématique d'Allemagne, où il donne un exposé systématique de tous les résultats importants connus jusque-là. Celui-ci est divisé en cinq parties: (1) Théorie générale, (2) Extensions galoisiennes, (3) Corps quadratiques, (4) Corps cyclotomiques, (5) Corps kummériens et se termine par un chapitre sur le problème de Fermat. (Les corps kummériens signifient les extensions de la forme $K = k(\sqrt[m]{a})$ du corps k qui contient $\zeta_m = \exp(2\pi i/m)$.) Il couvre donc non seulement les Disquisitiones de Gauss d'un point de vue moderne mais aussi presque tous les travaux arithmétiques de Dirichlet, Kummer, Dedekind et autres. Il est à remarquer qu'il s'agit dans les parties (3), (4), (5) de sujets concernant les extensions abéliennes, dont Hilbert insiste sur l'importance dans l'Introduction de ce rapport. Le contenu de la partie (1) est dû essentiellement aux prédécesseurs de Hilbert tandis que celui de la partie (2) est une contribution de Hilbert lui-même. Il y considère en particulier ce qu'il a appelé les groupes de décomposition, d'inertie et de ramification d'un idéal premier $\bar{P}$ d'une extension galoisienne K sur k, définis comme suit (*cf.* Chevalley [2], Chap.2).

Le *groupe de décomposition* $G_D(\bar{P})$ d'un idéal premier $\bar{P}$ dans une extension galoisienne K/k avec le groupe de Galois $G(K/k)$ est le sousgroupe de $G(K/k)$ de ses éléments σ qui laissent $\bar{P}$ invariant: $\sigma(\bar{P}) = \bar{P}$. Supposons fixés K/k et $\bar{P}$ et notons pour simplifier $G = G(K/k)$, $G_D = G_D(\bar{P})$. Le sousgroupe G_D de G est d'indice g et d'ordre ef. Le *groupe d'inertie* $G_I(\bar{P})$ (ou G_I) de $\bar{P}$ est le sousgroupe de G_D (ou de G) des éléments τ tels que $\tau(\alpha) \equiv \alpha \pmod{\bar{P}}$ pour tout $\alpha \in A_K$. On a $(G_D : G_I) = f$, $|G_I| = e$. Pour un nombre naturel $\nu \geq 1$, on appelle $(\nu-1)$*-ième groupe de ramification* $G_{(\nu-1)}(\bar{P})$ (ou $G_{(\nu-1)}$) de $\bar{P}$ le sousgroupe de G_I (ou de G) des éléments τ tels que $\tau(\alpha) \equiv \alpha \pmod{\bar{P}^\nu}$ pour tout $\alpha \in A_K$. On a $G_I = G_{(0)} \supset G_{(1)} \supset \cdots \supset G_{(\mu)} = \{1\}$ pour un certain μ. Si $\bar{P}$ ne se ramifie pas, on a $G_I = \{1\}$, $\mu = 0$. On montre de plus que G_I est un sousgroupe invariant de G_D et que G_D/G_I est cyclique et engendré par $\sigma \in G_D$ tel que $\sigma(\alpha) \equiv \alpha^q \pmod{\bar{P}}$ où q est la norme absolu de P, l'idéal premier de k divisé par P. On appelle σ l'*automorphisme de Frobenius* de $\bar{P}$ (*cf.* Frobenius [1]). Les corps intermédiaires de K/k qui correspondent au sens de la théorie de Galois aux groupes de décomposition, d'inertie ou de ramification s'appellent d'après Hilbert les *corps de décomposition, d'inertie* ou *de ramification*.

Jusqu'ici on a considéré un idéal premier $\bar{P}$ de K comme fixé. Soit P l'idéal premier de k divisé par $\bar{P}$. L'idéal P peut avoir un autre diviseur premier $\bar{P}'$, qui est conjugué de $\bar{P}$ et peut être désigné par $\rho(\bar{P})$, $\rho \in G(K/k)$. On voit immédiatement que le groupe de décomposition de $\rho(\bar{P})$ est le sousgroupe conjugué $\rho G_D(\bar{P})\rho^{-1}$ de $G_D(\bar{P}) : G_D(\rho\bar{P}) = \rho G_D(\bar{P})\rho^{-1}$. Il en est de même pour les groupes d'inertie et de ramification et l'automorphisme de Frobenius. Si en particulier $G(K/k)$ est abélien, tous les sousgroupe conjugués ou même tous les éléments conjugués se coïncident. On peut donc parler alors des groupes de décomposition etc. et de l'automorphisme de Frobenius de P (au lieu de $\bar{P}$).

Hilbert a pu systématiser son exposé dans les trois dernières parties de son *Zahlbericht* à l'aide de cette théorie.

*

Hilbert parle du *corps de classes* dans un mémoire [3] sur les extensions quadratiques qu'il a publié peu de temps après son *Zahlbericht*, puis dans un autre mémoire intitulé: Sur la théorie des extensions abéliennes des corps de nombres algébriques [4], où il annonce les conjectures suivantes[2]:

Soit k un corps de nombres algébriques avec le groupe des classes C_k. Alors il existe une extension abélienne unique K de k jouissant des propriétés suivantes:

(i) *Le groupe de Galois $G(K/k)$ est isomorphe à C_k.*

(ii) *K/k n'est pas ramifié. (Par conséquent, aucun idéal premier de k n'est ramifié dans K).*

[2] Pour plus de simplicité, j'omets ici les considérations sur les classes d'idéaux au sens étroit pour le cas ou k est réel.

(iii) *Le type de décomposition dans K d'un idéal premier P de k dépend seulement de la classe d'idéaux de k à laquelle P appartient. Le degré f de P coïncide avec l'exposant de cette classe; c'est-à-dire P^f devient un idéal principal dans k tandis qu'aucune puissance de P avec un exposant inférieur ne devient principal*.

(iv) *Tout idéal de k transféré dans K devient principal*.

Hilbert a nommé cette extension K de k le *corps de classes* de k.

C'était des conjectures sûrement bien hardies pour Hilbert parce qu'il a pu les démontrer seulement dans le cas où $h_k = 2$, mais il en a été convaincu par leur beauté. Et heureusement toutes ces conjectures se sont révélées vraies! L'existence de l'extension K/k avec les propriétés (i)–(iii) a été démontrée par Furtwängler dans une série de travaux de 1907 à 1913 [1], et la quatrième propriété (iv) de K a été démontrée par lui en 1930 [2] plus de 15 ans plus tard.

Hilbert a pressenti quelques relations entre la théorie du corps de classes et la "loi de réciprocité" qui généraliserait la loi de réciprocité quadratique dont Gauss avait insisté sur l'importance. Le neuvième des problèmes mathématiques posés par Hilbert au Congrès à Paris en 1900 consista en la formulation et de la démonstration de cette loi de réciprocité, pour lesquelles, dit Hilbert, une généralisation appropriée des méthodes qu'il a données dans son mémoire sur les extensions quadratiques [3] serait utile.

Le 12$^{\text{e}}$ problème de Hilbert concerne aussi les extensions abéliennes des corps de nombres algébriques. Kronecker [1] avait conjecturé que toute extension abélienne de $\boldsymbol{Q}$ serait contenue dans un corps cyclotomique et que toute extension abélienne d'un corps quadratique imaginaire k serait obtenue par l'adjonction à k des "valeurs singulières" d'une certaine fonction elliptique. La première conjecture avait été démontrée par Weber [1], [4], et Hilbert [1] mais la seconde, connue sous le nom de *Jugendtraum* de Kronecker et dont la formulation n'était d'ailleurs pas précise, restait longtemps sans être élucidée, bien qu'elle ait été attaquée par de nombreux mathématiciens. Le problème a été posé par Hilbert sous une forme encore plus générale: trouver une fonction dont les "valeurs singulières" engendreraient les extensions abéliennes d'un corps de nombres algébriques donné. Hilbert dit qu'il le prend pour un des problèmes les plus profonds et d'une portée les plus grandes de la théorie des nombres et de la théorie des fonctions.

Ces deux problèmes de Hilbert, le 9$^{\text{e}}$ et le 12$^{\text{e}}$ au Congrès à Paris, paraîssent assez éloignés l'un de l'autre, mais tous les deux concernent les extensions abéliennes de corps de nombres algébriques, et Weber a remarqué dans un de ses travaux sur le second problème [2], un fait qui suggère une relation entre les deux.

*

Pour en parler, je commencerai par expliquer un peu plus la liaison entre les deux conjectures de Kronecker.

La première de celles-ci affirme que toute extension abélienne de $\boldsymbol{Q}$ est contenue dans une extension $\boldsymbol{Q}(\zeta_m)$, $\zeta_m = \exp(2\pi i/m)$, $m \in \boldsymbol{Z}$, $m \geq 1$. Si l'on pose $f(z) = \exp(2\pi iz)$, on a $f(z+1) = f(z)$, c'est-à-dire que $f(z)$ est une fonction automorphe pour le groupe additif de $\boldsymbol{C}$ engendré par $z \to z+1$ laissant $\boldsymbol{Z}$ invariant. On voit que toute extension abélienne de $\boldsymbol{Q}$ est contenue dans un corps engendré par une *valeur singulière* de cette fonction $f(z)$, c'est-à-dire par $f(r)$, $r \in \boldsymbol{Q}$.

Si l'on remplace $\boldsymbol{Q}$ par le corps de Gauss $\boldsymbol{Q}(i)$, l'anneau $\boldsymbol{Z}$ sera remplacé par $\boldsymbol{Z}[i]$, et la fonction $f(z) = \exp(2\pi iz)$ par la fonction de lemniscate, la fonction elliptique dont le parallélogramme de périodes coïncide avec le domaine fondamental du groupe additif de $\boldsymbol{Z}[i]$. On demande si toute extension abélienne du $k = \boldsymbol{Q}(i)$ est contenue dans une extension de k engendrée par une valeur singulière, c'est-à-dire valeur de cette fonction pour un élément de ce corps $\boldsymbol{Q}(i)$. Takagi a démontré dans sa Thèse [1] que la réponse à cette question est positive. On peut se poser la même question pour tout autre corps quadratique imaginaire. On a nommé cette question le problème de *multiplication complexe* parce que le réseau des entiers des corps quadratiques imaginaires admet un endomorphisme par multiplication par un entier complexe (par exemple multiplication par i dans le cas de $\boldsymbol{Z}[i]$.) La solution générale pour les corps quadratiques imaginaires a été également obtenue par Takagi [3]. Mais le problème 12 de Hilbert qui demande les fonctions génératrices des extension abéliennes de corps de nombres algébriques quelconques est encore loin d'être résolu malgré de brillants résultats par des mathématiciens comme Hecke [1], [2], Weil [11], Shimura [1], [2], [3], et Taniyama [1], Shimura–Taniyama [1] (*cf.* Serre [2]).

*

Soient k un corps de nombres algébriques (de degré fini), m un entier rationnel et $\zeta_m = \exp(2\pi i/m)$. L'extension $k(\zeta_m)$ de k s'appelle le *corps circulaire* (ou le *corps cyclotomique*) d'ordre m sur k. Si l'on a en particulier $k = \boldsymbol{Q}$, $\boldsymbol{Q}(\zeta_m)$ s'appelle le *corps circulaire absolu*. ζ_m est racine du *polynôme cyclotomique* $\Phi_m(X) \in \boldsymbol{Z}[X]$ de degré $\varphi(m)$, indicateur d'Euler représentant le nombre des entiers $\leq m$ qui sont relativement premiers à m; on a donc $(\boldsymbol{Q}(\zeta_m) : \boldsymbol{Q}) = \varphi(m)$ et on démontre que $\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q}$ est une extension abélienne dont le groupe de Galois $G(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})$ est isomorphe à $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$ et dont le discriminant se compose uniquement des diviseurs premiers de m. Si l'on désigne par E l'ensemble des diviseurs premiers de m, les nombres premiers en dehors de E ne se ramifient pas dans $\boldsymbol{Q}(\zeta_m)$. Si $p \notin E$, p appartient à une classe de $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$ et le type de décomposition de p dans $\boldsymbol{Q}(\zeta_m)$ ne dépend que de cette classe.

Ce qu'on a vu sur les corps circulaires absolus, se généralise aux corps circulaires en général. $k(\zeta_m)/k$ est une extension abélienne de groupe de Galois

isomorphe à un sousgroupe de $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$. Si E représente l'ensemble des idéaux premiers de k diviseurs de m, les idéaux premiers en dehors de E ne se ramifient pas dans $k(\zeta_m)$. Pour un idéal premier P de k en dehors de E, la loi de décomposition dans $k(\zeta_m)$ s'énonce comme suit: le degré relatif d'un diviseur premier $\overline{P}$ de P dans $k(\zeta_m)$ est égal à l'exposant de la classe de $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$ à laquelle $N_{k/\boldsymbol{Q}}(P)$ appartient. (Comme $P \notin E$, il est clair que $N_{k/\boldsymbol{Q}}(P)$ est relativement premier à m, et appartient donc à $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$.) On pourrait dire un peu sommairement que la loi de décomposition des idéaux premiers de k dans l'extension circulaire $k(\zeta_m)$ se détermine "par congruence mod m."(*cf.* Hilbert [2, Chap.IV], Chevalley [2, Chap.VII].) Et Weber [2] a remarqué qu'une loi de décomposition de même genre domine aussi dans les extensions qu'on rencontre dans la théorie de multiplication complexe.

*

Pour formuler plus exactement cette loi, il nous convient de parler d'abord des *valuations*, des *diviseurs* et des *rayons* modulo diviseurs dans un corps de nombres algébriques.

Soit d'abord k un corps quelconque. Une *valuation* φ de k signifie une application de k dans l'ensemble $\boldsymbol{R}^+$ des nombres réels non négatifs satisfaisant aux conditions suivantes:

1) $\varphi(a) = 0$ si et seulement si $a = 0$.

2) $\varphi(ab) = \varphi(a)\varphi(b)$.

3) $\varphi(a+b) \leq \varphi(a) + \varphi(b)$.

La notion de valuation généralise ainsi celle de la valeur absolue dans $\boldsymbol{R}$ ou $\boldsymbol{C}$. (Chevalley [2, Chap.V] utilise l'expression "valeur absolue" dans le sens de "valuation".) L'application φ définie par $\varphi(0) = 0$ et $\varphi : k^\times \to \{1\}$ est évidemment une valuation qui s'appelle la *valuation triviale*. Ce seront les valuations non triviales qui nous intéresseront dans ce qui suit.

Si k est un corps de nombres algébriques de degré fini avec r_1 conjugués réels $\sigma_i(k) = k^{(i)} \subseteq \boldsymbol{R}$, $i = 1, 2, \ldots r_1$ et $2r_2$ conjugués complexes $\sigma_{r_1+j}(k) = k^{(r_1+j)} \subseteq \boldsymbol{C}$ mais non $k^{(r_1+j)} \subseteq \boldsymbol{R}$, $\sigma_{r_1+r_2+j}(a) = \overline{\sigma_{r_1+j}(a)}$, $j = 1, 2, \ldots r_2$, k a évidemment $r_1 + r_2$ valuations $\varphi_h(a) = |\sigma_h(a)|$, $h = 1, 2, \ldots, r_1 + r_2$, où $|\ \ |$ désigne la valeur absolue habituelle dans $\boldsymbol{R}$ ou $\boldsymbol{C}$. Ces valuations satisfont à l'axiome d'Archimède: Si $a \neq 0$ et $n \in \boldsymbol{N}$, on a $\varphi(na) \to \infty$ quand $n \to \infty$. Celles-ci s'appellent les *valuations archimédiennes* de k.

En plus de ces $r_1 + r_2$ valuations, k a une infinité de *valuations non-archimédiennes* dont chacune correspond à un idéal premier P de k définies comme suit:

Soient P un idéal premier et A un idéal fractionnaire (non nul) de k. On écrira $e_P(A) = 0$ si P n'apparaît pas parmi les diviseurs premiers de A avec un exposant positif ou négatif. Autrement $e_P(A)$ signifiera cet exposant, c'est-à-dire $e_P(A) = \nu \in \boldsymbol{Z}$ si $e_P(P^{-\nu}A) = 0$ (ou bien si $P^\nu \| A$, ou bien encore si $P^\nu | A$, $P^{\nu+1} \nmid A$ comme on écrit habituellement.) Pour $a \in k^\times$, on pose $e_P(a) = e_P((a))$.

Soit c une constante réelle telle que $0 < c < 1$. Si l'on pose $\varphi_{P,c}(A) = c^{e_P(a)}$, pour $a \in k^\times$ et $\varphi_{P,c}(0) = 0$, $\varphi_{P,c} = \varphi$ est évidemment une valuation satisfaisant à

3′) $\varphi(a+b) \leq \mathrm{Max}(\varphi(a), \varphi(b))$

qui est plus fort que 3). Celle-ci est *non-archimédienne*.

Si c' est une autre constante avec $0 < c' < 1$, on trouve un ρ réel et positif tel que $c' = c^\rho$ et par conséquent $(\varphi_{P,c}(a))^\rho = \varphi_{P,c'}(a)$ pour tout a. On écrit alors $\varphi_{P,c'} = \varphi_{P,c}^\rho$ et appelle $\varphi_{P,c}$ et $\varphi_{P,c'}$ *valuations équivalentes*. A chaque classe de valuations équivalentes correspond un idéal premier P de k.

On démontre que pour un corps k de nombres algébriques de degré fini, les $r_1 + r_2$ valuations archimédiennes provenant des corps conjugués de k dans $\boldsymbol{C}$ et les valuations non-archimédiennes correspondant aux idéaux premiers de k sont les seules valuations possibles de k (Ostrowski [1], Artin [4], Chevalley [2, Chap.V]). Soit φ une valuation de k. On peut définir une métrique d_φ dans k en posant

$$d_\varphi(a,b) = \varphi(a-b)$$

et compléter k topologiquement par rapport à d_φ. Ces corps complétés $\bar{k}_\varphi$ s'appellent les *corps locaux*. Si φ est archimédienne, $\bar{k}_\varphi$ est topologiquement isomorphe à $\boldsymbol{R}$ ou à $\boldsymbol{C}$, et si φ est non-archimédienne, $\bar{k}_\varphi$ se détermine par P et s'appelle un *corps P-adique* noté k_P.

Les valuations équivalentes définissent la même topologie de k. Chaque classe d'équivalence de valuations de k définit une *place* de k dite *finie* ou *infinie* selon que les valuations envisagées sont non-archimédiennes ou archimédiennes. Chaque place finie est représentée par un idéal premier P de k. Pour représenter les places infinies, Hasse [2] a introduit les symboles des *idéaux à l'infini* $P_{\infty,1}, \ldots, P_{\infty,r_1}, P_{\infty,r_1+1}, \ldots, P_{\infty,r_1+r_2}$ correspondant aux corps conjugués $k^{(1)}, \ldots, k^{(r_1)}$, $k^{(r_1+1)}, \ldots, k^{(r_1+r_2)}$ dont les r_1 premiers sont réels.

On définit maintenant un *diviseur* M dans k par un produit formel d'un ensemble fini de places finies ou infinies réeles de k:

$$(*) \qquad M = P_1^{e_1} \cdots P_g^{e_g},$$

avec des exposants $e_i \in \boldsymbol{N}$, $i = 1, 2, \ldots, g$ assujettis aux conditions: $e_i > 0$ ou $= 1$ selon que P_i est fini ou infini réel. On appellera $(*)$ la *décomposition* de M, les P_i qui y figurent (avec les exposants $\neq 0$) les *facteurs* de M, et notera $E(M)$ l'ensemble de ces facteurs. Si $P \in E(M)$, $e_P(M)$ désignera l'exposant de P dans la décomposition de M, et si $P \notin E(M)$ on posera $e_P(M) = 0$. On admettra aussi le diviseur $M = 1$, pour lequel $e_P(M) = 0$ pour toute place P de k, finie ou infinie.

Pour deux diviseurs M, M' de k, on dira "M divise M'" et écrira $M \mid M'$ si $e_P(M) \leq e_P(M')$ pour toutes les places P de k. L'ensemble de ces diviseurs est évidemment partiellement ordonné par cette relation d'ordre. Le diviseur 1 est le minimum de tous ces diviseurs, et on peut naturellement parler du p.g.c.d. (M, M') et du p.p.c.m $[M, M']$ des deux diviseurs.

Soit $\mathfrak{P}$ l'ensemble de tous les idéaux premiers de k (qui peut s'identifier avec toutes les places finies de k.) M étant un diviseur donné, posons $E_0(M) = E(M) \cap \mathfrak{P}$, $M_0 = \prod_{P \in E_0(M)} P^{e_P(M)}$ et appelons M_0 la *partie finie* de M. On a évidemment $M_0 \mid M$ et peut poser $M = M_0 M_\infty$ avec un autre diviseur M_∞ (pour lequel on a $(M_\infty)_0 = 1$) qu'on appellera la *partie infinie* de M. On dit qu'un diviseur M est *fini* ou *infini* selon que $M_\infty = 1$ ou $M_0 = 1$.

Si A est un idéal entier ($\neq 1$) de k, A se représente comme un produit des puissances d'idéaux premiers avec des exposant positifs. Il s'identifie ainsi avec un diviseur fini. Pour $a \in k^\times$, l'idéal fractionnaire (a) se représente comme AB^{-1} avec deux idéaux entiers A, B relativement premiers. On dit qu'un diviseur fini M_0 divise a, et écrit $M_0 \mid a$, si $M_0 \mid A$ et $(M_0, B) = 1$.

Pour deux éléments $a, b \in k^\times$ et un diviseur $M = M_0 M_\infty$, on définit la *congruence multiplicative*

$$a \equiv b \pmod{M}$$

par deux conditions: 1) $M_0 \mid ab^{-1}$ et 2) $\sigma_i(a)$ et $\sigma_i(b)$ ont la même signature (c'est-à-dire $\sigma_i(ab) > 0$) si $P_{\infty,i} \mid M_\infty$. (Rappelons que M_∞ ne contient que des places à l'infini réelles.) M étant un diviseur donné, on montre facilement que l'ensemble des idéaux principaux (a) avec $a \in k^\times$, satisfaisant à $a \equiv 1 \pmod{M}$ forme un sousgroupe (multiplicatif) d'indice fini du groupe F^E de tous les idéaux relativement premiers aux idéaux premiers dans E (Pour simplifier, nous dirons dorénavant: les idéaux de F^E sont relativement premiers à E.) où $E = E(M)$. On appellera ce groupe le *rayon* mod M et le notera R_M. On voit sans peine $R_{(M,M')} = [R_M, R_{M'}]$ (le sousgroupe de F^E engendré par R_M et $R_{M'}$) et $R_{[M,M']} = R_M \cap R_{M'}$, M, M' étant deux diviseurs quelconques de k.

*

Soient k un corps de nombres algébriques, M, M' des diviseurs de k, $E = E(M)$ et $E' = E(M')$. Un sousgroupe H_M de F^E contenant R_M s'appelle *un groupe d'idéaux définissable* mod M et M un *module de définition* de H_M. Si $M \mid M'$, on a $E \subset E'$, $F^E \supset F^{E'}$, $R_M \supset R_{M'}$ et pour un groupe d'idéaux H_M, son sousgroupe $(H_M)^{E'}$ constitué des idéaux qui sont relativement premiers à E', devient un groupe d'idéaux $H_{M'}$ définissable mod M', pour lequel on a $F^E/H_M \cong F^{E'}/H_{M'}$. Dans ce sens on dit qu'un groupe d'idéaux définissable mod M est définissable aussi mod M' pour un diviseur M' divisible par M, et on identifie F^E/H_M et $F^{E'}/H_{M'}$. Soient M, M' deux diviseurs et posons $[M, M'] = M''$. Si H_M et $H_{M'}$ s'identifient au même $H_{H''}$ dans le sens susdit, on écrira $H_M \approx H_{M'}$. Ceci définit comme il est facile de voir, une relation d'équivalence entre les groupes d'idéaux définissables mod différents diviseurs de k. Si $H_M, H'_M, \ldots$ sont des groupes d'idéaux avec différents modules de définition $M, M', \ldots$ appartenant à une même classe d'équivalence, on voit que le p.g.c.d. $(M, M', \ldots)$ est aussi un module de définition d'un groupe d'idéaux de la même classe.

Cette classe a donc un module de définition minimum qui s'appellera le *conducteur* C de cette classe, qui se représentera par H_C, groupe d'idéaux définissable mod C. Dorénavant on représentera toujours (sauf mention expresse) un groupe d'idéaux $H_M \bmod M$ par le groupe d'idéaux $H_C \bmod C$, C étant son conducteur tel que $H_M \approx H_C$. Soient $H = H_C$ un groupe d'idéaux donné et E l'ensemble des idéaux premiers diviseurs de C. Les éléments du groupe quotient F^E/H s'appelleront les *classes d'idéaux* $\bmod H$, ce groupe quotient le *groupe de ces classes*, le cardinal de ce groupe le *nombre des classes* $\bmod H$. (Sans préciser H, on appelle parfois *classes par congruence* les classes d'idéaux mod certain H, H étant un groupe d'idéaux définissable mod certain diviseur M.) On remarquera que le rayon mod 1 n'est autre chose que le groupe des idéaux principaux, et les classes d'idéaux mod 1 coïncident avec les classes d'idéaux habituelles dont on a parlé plus haut. De plus, soient $\boldsymbol{Q}$ le corps des rationnels, m un entier positif, p_∞ l'unique idéal à l'infini de $\boldsymbol{Q}$ est $M = mp_\infty$. Alors le groupe des classes $\bmod R_M$ est isomorphe à $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$: Si l'on écrit donc $F = \boldsymbol{Q}^\times$, $E = E(M)$, $H = R_M$, on a $F^E/H \cong (\boldsymbol{Z}/m\boldsymbol{Z})^\times = G(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})$ et le type de décomposition des nombres premiers $p \notin E$ dans $\boldsymbol{Q}(\zeta_m)$ dépend seulement de la classe de F^E/H à laquelle p appartient.

*

L'idée de généraliser ainsi la notion des classes d'idéaux qui avait été déjà conçue par Weber [2] a été utilisée par Takagi dans son travail [1] où il a traité la théorie des extensions abéliennes du corps de Gauss $\boldsymbol{Q}(i)$. Peut-être en a-t-il déjà pressenti alors la grande signification pour la théorie générale des extensions abéliennes des corps de nombres algébriques? Après avoir étudié trois semestres à Göttingen auprès de Hilbert, il est retourné au Japon en 1901 et s'est mis à en faire des recherches profondes jusqu'à l'époque de la Première Guerre Mondiale. Il faut se rappeler qu'à cette époque Furtwängler avait déjà établi la validité des conjectures de Hilbert sur le corps de classes (sauf (iv)). A ce stade, il était donc assez naturel de penser à la généralisation suivante des conjectures de Hilbert.

Soit $H = H_C$ un groupe d'idéaux de conducteur C dans un corps de nombres algébriques k de degré fini, de groupe de classes d'idéaux F^E/H, où E est l'ensemble des idéaux premiers diviseurs de C. Alors il existe une extension abélienne unique K de k jouissant des propriétés suivantes:

(i) *Le groupe de Galois $G(K/k)$ est isomorphe à F^E/H.*

(ii) *Tout idéal premier en dehors de E n'est pas ramifié.*

(iii) *Le type de décomposition de $P \notin E$ dépend seulement de la classe de F^E/H à laquelle P appartient. Le degré f de P coïncide avec l'exposant de cette classe.*

(En ce qui concerne un analogue de (iv) des conjectures d'Hilbert, p.32, je le laisse en suspens ici. J'y reviendrai vers la fin de cette Introduction, p.77)

Il est naturel d'appeler cette extension K de k le *corps de classes associé à* H. Pour le cas de $C = 1$, $H = R_1$ (le rayon mod 1, c'est-à-dire le groupe des idéaux principaux), cette notion coïncide avec celle de Hilbert, et pour le cas de $k = \boldsymbol{Q}$ et $H = R_{mp_\infty}$, on a $K = \boldsymbol{Q}(\zeta_m)$ pour lequel tout s'accorde! Et Takagi a eu le premier l'idée de soupçonner:

(iv) *Toute extension abélienne de k est le corps de classes associé à un groupe d'idéaux* $H = H_C$ *pour un certain* C.

Et Takagi a réussi à démontrer dans son travail [3] que toutes ces "conjectures" sont vraies! (Hasse [2] a appelé cette dernière proposition (iv) le *théorème réciproque* (*Umkehrsatz*) de la théorie du corps de classes.)

*

Rappelons-nous ici des précurseurs de la théorie du corps de classes avant Hilbert (*cf.* Hasse [10]).

Kronecker avait déjà parlé assez longuement dans son mémoire célèbre sur la théorie arithmétique des quantités algébriques [2] d'une extension K d'un corps de nombres algébriques k où tous les idéaux de k deviennent principaux. Dans notre langage, il parlait ainsi du corps de classes au sens de Hilbert. Son attention a été surtout attirée par la propriété (iv) de ce corps, dont Furtwängler [2] a pu vérifier la validité ultérieurement, mais on reconnait maintenant, que ce n'est pas là une propriété appropriée comme la base de la théorie (*cf.* infra p.78).

Un autre précurseur était H. Weber qui a défini dans ses mémoires [1], [2] ce que nous appelons maintenant les groupes d'idéaux pour exprimer la loi de décomposition dans les extensions abéliennes K qu'on rencontre dans la théorie de multiplication complexe. Une telle extension K/k étant donnée, il a remarqué qu'il y a un groupe d'idéaux H dans k, tel que l'ensemble des idéaux premiers de k qui se décomposent complètement dans K coïncide avec l'ensemble des idéaux premiers qui appartiennent à H. Weber [1] a donné la définition suivante du corps de classes, suggéré par cette situation, pour un groupe d'idéaux H dans un corps de nombres algébriques k: c'est une extension K de k pour laquelle la loi de décomposition des idéaux premiers ci-dessus est valable. Weber a montré qu'il n'y qu'un seul corps de classes pour le groupe d'idéaux H donné, et que si K_1, K_2 sont les corps de classes pour deux groupes d'idéaux H_1, H_2, respectivement, $K_1 \subset K_2$ et $H_1 \supset H_2$ s'entraînent mutuellement. Il n'a pas démontré l'existence du corps de classes pour un groupe d'idéaux H donné, mais il s'en était sûrement convaincu, comme l'introduction de son mémoire [1] l'indique, dit Hasse [10]. Sous l'hypothèse de l'existence de ce corps, il a démontré l'existence d'une infinite d'idéaux premiers dans chacune des classes F^E/H. Dans ces considération, Weber a utilisé la méthode analytique par laquelle Dirichlet avait démontré le "théorème de la progression arithmétique." (En fait ce théorème, qui dit qu'il y a une infinité de nombres premiers dans la suite

$a+nb, n=1,2,\ldots$, si $(a,b)=1$, n'est autre chose que l'affirmation que chaque classe de $(\boldsymbol{Q}^\times)^E/R_{bp_\infty}$ où E est l'ensemble des diviseurs premiers de b, contient une infinité de nombres premiers.)

Ces mémoires de Weber ont directement influencé Takagi, quand celui-ci a entrepris de réfléchir sur cette théorie. Lorsqu'il a réussi à l'établir dans [3], il l'a construite en partant d'une définition du corps de classes inspirée par un résultat analytique de Weber que j'expliciterai tout à l'heure.

Ces méthodes analytiques ont sûrement paru à Chevalley, algébriste tenant à la pureté des méthodes, comme essentiellement étrangères à la théorie éminemment arithmétique du corps de classes. Déjà sa première contribution en collaboration avec Herbrand [2] l'indique. Il essaya de l'éliminer dans sa Thèse [2], mais n'y réussit pas tout à fait; il y réussit dans [3] en 1935 en collaboration avec Nehrkorn, puis enfin dans [6] en 1940. Dans sa Thèse, il a pu réduire le problème à celui de montrer que les corps circulaires sont corps de classes (en un sens qui sera précisé plus loin), et dans son mémoire [6], il a atteint son but en prouvant un autre théorème d'existence pour les idéaux premiers, mais il faut reconnaître que la théorie de Chevalley ne contient pas le "théorème général de la progression arithmétique", c'est-à-dire l'affirmation de l'existence d'une infinité d'idéaux premiers dans chaque classe de F^E/H.

L'histoire nous fait voir que la méthode analytique a servi essentiellement à la genèse et au développement de cette théorie. Je consacrerai donc encore les paragraphes suivants à l'exposé de cette méthode.

*

On sait qu'Euclide avait déjà démontré l'existence d'une infinité de nombres premiers et il est facile de montrer par le même argument qu'il en est de même pour les nombres premiers de la forme $4m-1$ ou $6m-1$, mais cela ne marche plus pour ceux de la forme $4m+1$ ou $6m+1$. Euler a conçu un nouveau moyen pour rétablir le résultat d'Euclide en envisageant l'identité

$$(*) \qquad \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1-p^{-s})^{-1}$$

où p parcourt l'ensemble de tous les nombres premiers. Cette identité équivaut au théorème fondamental de l'arithmétique élémentaire que tout entier rationnel s'exprime d'une manière unique comme produit de nombres premiers. Euler a considéré cette identité formelle pour $s=1$ et raisonné comme suit: si l'ensemble de nombres premiers était fini, le second membre de cette identité serait fini tandis que le premier membre est infini, ce qui n'est pas. On peut justifier ce raisonnement en considérant les deux membres avec le paramètre $s \in \boldsymbol{R}, s>1$ et laissant s tendre vers 1. Plus tard, Riemann [1] a considéré la valeur de $\sum_{n=1}^{\infty} \frac{1}{n^s}$

comme une fonction de variable complexe s qu'il a notée $\zeta(s)$, prolongeable analytiquement dans le plan entier $s \in \boldsymbol{C}$, avec un seul pôle à $s = 1$ avec le résidu 1, satisfaisant à une équation fonctionnelle bien connue, et encore plus tard, Hadamard [1] et de la Vallée-Poussin [1] ont démontré presque simultanément et indépendamment le célèbre "théorème des nombres premiers" disant que le nombre $\pi(x)$ des nombres premiers ne dépassant pas $x \in \boldsymbol{R}$ satisfait à l'équation asymptotique

$$\lim_{x\to\infty} \pi(x) \Big/ \frac{x}{\log x} = 1,$$

en utilisant les résultats de la théorie des fonctions entières d'une variable complexe. (Il est bien connu aussi que Riemann a énoncé dans [1] son hypothèse sur les zéros de la fonction $\zeta(s)$, qui reste encore non-résolue.) On appelle maintenant les *fonctions zêta* les différents genres de fonctions généralisant la fonction $\zeta(s)$ dit de Riemann définie comme plus haut. Toutes ces fonctions admettent des représentations comme *produits eulériens* liés aux règles multiplicatives des entités en considération comme produits des "entités premières", dont le comportement de ces fonctions autour d'un pôle (qui se trouve à $s = 1$ pour $\zeta(s)$ de Riemann) indique la "densité", dont on donnera plus tard une définition précise (*cf.* infra p.44).

Pour un corps de nombres algébriques k (de degré fini $n = (k : \boldsymbol{Q})$), Dedekind [1] a défini la *fonction zêta de* k par

$$\zeta_k(s) = \sum \frac{1}{NA^s}$$

où A parcourt tous les idéaux entiers de k, et N désigne la norme de k à $\boldsymbol{Q}$. Elle admet une représentation en produit eulérien

$$\zeta_k(s) = \prod_P (1 - NP^{-s})^{-1},$$

où P parcourt tous les idéaux premiers de k.

Soit maintenant E un ensemble fini d'idéaux premiers de k. Si l'on enlève tous les idéaux A figurant dans la somme $\sum \frac{1}{NA^s}$ de la définition de $\zeta_k(s)$ ceux qui ont des facteurs premiers appartenant à E, on obtient une fonction $\zeta_k^E(s) = \sum^E \frac{1}{NA^s}$ qui admet une représentation comme produit eulérien $\prod^E (1 - NP^{-s})^{-1}$, où $\prod^E$ indique que P parcourt tous les idéaux premiers en dehors de E.

*

Soient maintenant M un diviseur de k, E l'ensemble des idéaux premiers facteurs de M, F^E le groupe de tous les idéaux de k relativement premiers à E et H un groupe d'idéaux définissable mod M. Posons $\Phi = F^E/H = \{c_1, c_2, \ldots, c_h\}$

avec $c_1 = H$; c'est un groupe abélien fini d'ordre h qui est le nombre des classes d'idéaux mod H. Soit $\widehat{\Phi} = \{\chi; \chi(\Phi) \in \boldsymbol{C}, |\chi(c_i)| = 1, i = 1, \ldots, h\}$ *le groupe des caractères* de Φ (*cf.* Chevalley [2] Chap.1). On sait $|\widehat{\Phi}| = |\Phi| = h$, de sorte qu'on peut écrire $\widehat{\Phi} = \{\chi_1, \chi_2, \ldots, \chi_h\}$ où χ_1 est le *caractère principal* (c'est-à-dire que $\chi_1(c_i) = 1$, $i = 1, \ldots, h$). On a de plus les *relations d'orthogonalité*:

$$\sum_{i=1}^{h} \chi_i(c_j) = \begin{cases} h & j = 1, \\ 0 & j \neq 1, \end{cases} \qquad \sum_{j=1}^{h} \chi_i(c_j) = \begin{cases} h & i = 1 \\ 0 & i \neq 1. \end{cases}$$

Tout idéal $A \in F^E$ appartient à une classe $c \in \Phi$, qu'on écrira $c(A)$. Pour $\chi \in \widehat{\Phi}$, $A \in F^E$, on posera $\chi(A) = \chi(c(A))$ et définira

$$(**) \qquad L(s, \chi, H) = \sum_A^E \frac{\chi(A)}{N(A)^s} = \prod_P^E (1 - \chi(P)N(P)^{-s})^{-1}$$

où les sens de $\sum_A^E$, $\prod_P^E$ sont clairs d'après ce qui précède. L'égalité du deuxième et du troisième membres suit immédiatement de $\chi(AB) = \chi(A)\chi(B)$ pour $A, B \in F^E$.

La fonction ainsi définie $L(s, \chi, H)$ est aussi une des fonctions zêta, comme elle se représente par un produit eulérien. Elle a été introduite par Dirichlet pour le cas $k = \boldsymbol{Q}, H = R_{mp_\infty}$ pour démontrer le théorème de la progression arithmétique. Le cas général a été traité par Hecke [3], mais on peut en trouver l'idée d'origine chez Dirichlet [1]. Remarquons que pour $k = \boldsymbol{Q}$, $\chi = \chi_1$, $H = \{1\}$, la fonction $L(s, \chi, H)$ coïncide avec $\zeta_k(s)$.

On appelle une *série de Dirichlet* toute série de la forme $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ où $a_n \in \boldsymbol{C}$. Elle converge évidemment si les $|a_n|$ sont bornés et la partie réelle σ de s est > 1 et y représente une fonction holomorphe de s. $L(s, \chi, H)$ en est évidemment une.

En prenant le logarithme de $(**)$, on obtient

$$\begin{aligned} \log L(s, \chi, H) &= -\sum_P^E \log\left(1 - \frac{\chi(P)}{N(P)^s}\right) \\ &= \sum_P^E \frac{\chi(P)}{N(P)^s} + \frac{1}{2}\sum_P^E \frac{\chi(P)^2}{NP^{2s}} + \cdots \end{aligned}$$

où $\frac{1}{2}\sum \frac{\chi(P)^{2s}}{N(P)^{2s}} + \cdots$ est une série de Dirichlet qui converge pour $\sigma > \frac{1}{2}$, donc est régulière pour $s = 1$. Et aussi dans la série $\sum \frac{\chi(P)}{N(P)^s}$ la somme des termes avec $NP = p^f$, $f \geq 2$ est régulière pour $s = 1$ pour la même raison.

On a déjà vu qu'Euler a démontré l'existence d'une infinité de nombres premiers en se basant sur le comportement de la fonction $\zeta(s)$ en $s = 1$. Nous

utiliserons des raisonnements de même nature pour établir l'existence d'une infinité d'idéaux premiers dans différents ensembles donnés. Pour faire ressortir ce qui nous compte dans ces raisonnements, nous écrivons $f(s) \sim g(s)$ pour deux fonctions analytiques $f(s), g(s)$ définies autour de $s = 1$ qui y ont le même comportement, c'est-à-dire que la différence $f(s) - g(s)$ reste régulière à $s = 1$. Dans cette notation, on peut écrire

$$(***) \qquad \log L(s, \chi, H) \sim \sum_P^{E\ 1} \frac{\chi(P)}{NP^s}$$

où $\sum_P^{E\ 1}$ signifie que P parcourt seulement les idéaux premiers de degré premier en dehors de E.

Si en particulier $\chi = \chi_1$, on a évidemment

$$\log L(s, \chi_1, H) \sim \log \zeta_k(s) \sim \log \frac{1}{s-1}$$

de sorte qu'on a en vertu de $(***)$

$$\log \frac{1}{s-1} \sim \sum_P^{E\ 1} \frac{1}{NP^s}$$

ce qui assure l'existence d'une infinité d'idéaux premiers de premier degré dans k.

En additionnant les formules $(***)$ en faisant χ parcourir tous les éléments de $\widehat{\Phi}$, on obtient

$$\sum_{\chi \in \hat{\Phi}} \log L(x, \chi, H) \sim h \sum_{P \in H}^{E\ 1} \frac{1}{NP^s}$$

en vertu des relations d'orthogonalité.

On sait que $L(s, \chi, H)$ est une fonction entière pour $\chi \neq \chi_1$. Si $L(1, \chi) \neq 0$ pour $\chi \neq \chi_1$, on aura $\log L(s, \chi, H) \sim 0$ pour $\chi \neq \chi_1$, d'où

$$\sum_{P \in H}^{E\ 1} \frac{1}{NP^s} \sim \frac{1}{h} \log \frac{1}{s-1},$$

assurant l'existence d'une infinité d'idéaux premiers de premier degré dans H. Si $L(1, \chi_i, H) = 0$, soit $\nu_i \in \boldsymbol{N}$ tel que $(s-1)^{-\nu_i} L(s, \chi_i, H) \neq 0$ pour $s = 1$. On aura alors

$$\log L(s, \chi_i, H) \sim -\nu_i \log \frac{1}{s-1}$$

d'où

$$\left(1 - \sum_{i=2}^{h} \nu_i\right) \log \frac{1}{s-1} \sim h \sum_{P \in H}^{E\ 1} \frac{1}{NP^s}.$$

Quand s prend une valeur réelle >1 et tend vers 1, le second membre est positif, de sorte que $\sum_{i=1}^{h} v_i$ doit être ≤ 1. Donc il n'y a qu'un seul v_i qui peut être >0, dans lequel cas les autres v_i doivent être 0. Il n'y a donc que deux possibilités pour la limite

$$\lim_{s\to 1}\left(\sum_{P\in H}{}^{E}{}_{1}\frac{1}{NP^s}\Big/\log\frac{1}{s-1}\right).$$

Elle est $1/h$ si $L(1,\chi_i)\neq 0$ pour $i=2,\ldots,h$; sinon elle est 0. (Dans ce deuxième cas, il n'y a qu'un seul $i\in\{2,3,\ldots,h\}$ pour lequel $L(1,\chi_i)=0$, et pour cette valeur de i on aura $(s-1)^{-1}L(s,\chi_i)\neq 0$.)

Weber a montré que l'existence du corps de classes pour H assure que le deuxième cas ne peut avoir lieu, et Takagi a établi en 1915 [2] l'existence de ce corps de classes. (Un peu plus tard en 1917, Hecke [3] a montré analytiquement $L(1,\chi_i)\neq 0$.) Avant d'expliquer le raisonnement de Weber, nous remarquerons que le fait $L(1,\chi_i,H)\neq 0$, $i=2,3,\ldots,h$ entraîne aussi l'existence d'une infinité d'idéaux premiers dans chaque classe $c_2,c_2,\ldots,c_h$.

Soit en effet $c\in\{c_1,c_2,\ldots,c_h\}=F^E/H$. En multipliant par $\chi(c^{-1})$ chaque formule de $(***)$, et en additionnant toutes ces formules, on obtient

$$\sum_{P}{}^{E}{}_{1}\frac{\chi(c^{-1})\chi(P)}{NP^s}\sim\sum_{\chi}\chi(c^{-1})\log L(s,\chi,H)$$

d'où, en vertu des relations d'orthogonalité,

$$h\sum_{P\in c}{}^{E}{}_{1}\frac{1}{NP^s}\sim\log\frac{1}{s-1}.$$

Tous ces résultats nous motivent à définir la *densité* $d(\mathscr{E})$ des idéaux premiers dans un ensemble $\mathscr{E}$ par

$$d(\mathscr{E})=\lim_{s\to 1}\left(\sum_{P\in\mathscr{E}}\frac{1}{NP^s}\right)\Big/\log\frac{1}{s-1}.$$

Ainsi on a $d(\mathscr{E})=1/h$ pour $\mathscr{E}\in\{c_1,\ldots,c_h\}$, ce qu'on pourrait exprimer en disant que les idéaux premiers sont *distribués avec une densité égale* dans chacune des classes mod H. (Chaque ensemble avec densité positive contient une infinité d'idéaux premiers. La densité ne change pas, si l'on élimine les idéaux premiers de degré ≥ 2. Il est évident que $\mathscr{E}\supset\mathscr{E}'$ entraîne $d(\mathscr{E})\geq d(\mathscr{E}')$.)

*

Pour faire voir que l'existence d'un corps de classes pour H entraîne $L(1,\chi_i,H)\neq 0$ pour $i=2,\ldots,h$, Weber a pris le biais suivant.

Soient K/k une extension galoisienne de degré n, $(K:k)=n$, et $\mathscr{E}_1$ l'ensemble des idéaux premiers de k qui se décomposent complètement dans K. On va montrer $d(\mathscr{E}_1)=1/n$. On obtient d'abord

$$\sum_{\bar{P}} \frac{1}{\bar{N}(P)^s} \sim \log \frac{1}{s-1}$$

où $\bar{P}$ parcourt les idéaux premiers du degré premier de K et $\bar{N}$ signifie la norme absolue $N_{K/\boldsymbol{Q}}$, du comportement de $\zeta_K(s)$ autour de $s=1$. Si l'on pose $N_{K/k}(\bar{P})=P$, on a $P=\prod_{i=1}^{n}\bar{P}^{\sigma_i}$, où $G(K/k)=\{\sigma_1,\ldots,\sigma_n\}$. Le premier membre de la dernière formule peut s'écrire donc $n\sum_{P}{}^{1}\frac{1}{N(P)^s}$, où P parcourt les idéaux premiers de $\mathscr{E}_1$ de degré premier et N signifie $N_{k/\boldsymbol{Q}}$. On a donc $d(\mathscr{E}_1)=1/n$.

Supposons maintenant l'existence du corps de classes K au sens de Weber associé à un groupe d'idéaux H dans k. L'ensemble $\mathscr{E}_1$ des idéaux premiers de k qui se décomposent complètement dans K coïncide alors avec l'ensemble $\mathscr{E}$ des idéaux premiers dans H. Par le même raisonnement que plus haut, on a $d(\mathscr{E})=1/n$, où $n=(K:k)$. On a vu d'autre part qu'il n'y a que deux possibilités pour la valeur de $d(\mathscr{E})$: soit $1/h$ ou 0 selon que $\prod_{i=2}^{h}L(1,\chi_i,H)\neq 0$ ou $=0$. Mais $\mathscr{E}_1=\mathscr{E}$ exclut ce deuxième cas, d'où s'ensuit $d(c)=1/h$, pour $c\in\{c_1,c_2,\ldots,c_h\}$.

*

A une extension galoisienne K/k de degré n et un module M de k, on associe un groupe d'idéaux $H(K,M)$ définissable mod M de la manière suivante: $H(K,M)$ est le sousgroupe de F^E où $E=E(M)$, engendré par R_M et $N_{K/k}(\bar{A})$, $\bar{A}$ étant les idéaux de K relativement premiers à M. Chevalley a nommé plus tard ce groupe $H(K,M)$ le *groupe de Takagi* dans k associé à K mod M. (En fait, il avait été ainsi déjà envisagé par Weber [2].) Comme on a $F^E\supset H(K,M)\supset R_M$, $H(K,M)$ a un indice fini $h(K,M)$ dans F^E, et d'après ce qu'on a vu plus haut pour les groupes d'idéaux en général, on a $d(H(K,M))=1/h(K,M)$. Or, il est évident que $H(K,M)$ contient tous les idéaux premiers (en dehors de E) qui se décomposent complètement dans K. L'ensemble de ces derniers idéaux a été noté $\mathscr{E}_1$, et on a montré $d(\mathscr{E}_1)=1/n$, d'où s'ensuit $1/h(K,M)\geq 1/n$, ou $h(K,M)\leq n$.

L'extension galoisienne K/k étant donnée, le groupe $H(K,M)$ et son indice $h(K,M)$ dépendent du module M. Il est clair que $M_1|M_2$ entraîne $H(K,M_1)\supset H(K,M_2)$ donc $h(K,M_1)\leq h(K,M_2)$, ce qu'on pourrait exprimer en disant que l'indice $h(K,M)$ "grandit avec M." Mais comme on a vu que cet indice est borné par $n=(K:k)$, il y a la valeur maximum de $h(K,M)$ pour tout choix de M, et un module M déterminé par K pour lequel $h(K,M)$ "devient maximal" et $H(K,M)$ "devient minimal." Soit M_0 le module ainsi déterminé. On appellera alors $H(K,M_0)$ le groupe d'idéaux de k associé à K et le notera $H(K)$

ou $H(K/k)$ parce qu'il se détermine par K/k. Et on appellera le conducteur du groupe $H(K) = H(K/k)$ le *conducteur de* K ou de K/k.

Takagi [3] a eu l'idée d'introduire une nouvelle définition du corps de classes associé à H en affaiblissant la définition de Weber comme suit:

Soient H un groupe d'idéaux dans k et K/k une extension galoisienne. On appellera K un corps de classes associé à H si $H = H(K)$ et son indice $h = h(K) = h(K,C)$ où C est le conducteur de H, coïncide avec $n = n(K) = (K : k)$.

On a démontré analytiquement qu'on a en géneral

$$\text{(I)} \qquad h(K) \leq n(K)$$

pour toute extension galoisienne K/k. On appelle cette inégalité la *première inégalité* et l'inégalité opposée

$$\text{(II)} \qquad h(K) \geq n(K)$$

la *deuxième inégalité* dans la (vieille) théorie du corps de classes. Takagi a appelé une extension galoisienne K de k un corps de classes sur k si

$$\text{(III)} \qquad h(K) = n(K),$$

c'est-à-dire que si la deuxième inégalité a lieu aussi. (Pour simplifier la locution, nous nous permetterons de dire en dépit d'une petite contravention grammaticale, que "*K/k est un corps de classes*" quand (III) a lieu pour une extension galoisienne K/k.)

Il est évident qu'un corps de classes au sens de Weber l'est aussi au sens de Takagi. Plus tard on verra que la réciproque est vraie, que le corps de classes au sens de Takagi a toutes les propriétés mentionnées plus haut, et de plus que toutes les extensions abéliennes sont les corps de classes, et pour tout groupe d'idéaux donnée H dans k, il existe un corps de classes qui lui est associé.

D'un autre côté, la méthode analytique exposée plus haut nous fait voir facilement que l'existence du corps de classes associé à H suffit pour la démonstration de $\prod_{i=2}^{n} L(1,\chi_i,H) \neq 0$, qui implique la positivité de la densité de toutes les classes $c_1, c_2, \ldots, c_h \bmod H$.

*

On voit que cette "nouvelle définition" du corps de classes introduite par Takagi: l'extension K/k est corps de classes si elle est galoisienne et $h(K) = n(K)$, a été évidemment motivée par les idées analytiques. Un peu plus loin, on va voir qu'une des raisons qui ont conduit Artin à sa "loi générale de réciprocité" a été sa préoccupation aux bons comportements de la "nouvelle espèce de séries L" qui concerne aussi les idées analytiques, idées qui devront être éliminées par Chevalley. On voit qu'elles ont pourtant joué les rôles si importants dans la genèse de notre théorie, ce qui montrera, d'un autre côté, la force de l'idée de la

purification conçue par Chevalley. Pour encore un certain temps, je continuerai d'expliquer ce qui a été fait par Takagi et Artin, utilisant les idées analytiques, avant d'aborder de parler des propres travaux de Chevalley.

*

La "nouvelle définition" de Takagi facilite beaucoup l'établissement de la théorie. D'après cette définition, il est d'abord facile de démontrer le *théorème d'ordre*: Soient H_1, H_2 deux groupes d'idéaux dans k, et K_1, K_2 corps de classes sur k associés à H_1, H_2. Alors $H_1 \subset H_2$ et $K_1 \supset K_2$ s'entraîne mutuellement, d'où s'ensuit le *théorème d'unicité*: Pour un groupe d'idéaux H donné, il n'y a qu'un seul corps de classes K. Ce résultat peut se préciser aisément comme le *théorème d'intersection et de composition*: Soient K_1, K_2 corps de classes associés à H_1, H_2. Alors le corps d'intersection $K_1 \cap K_2$ et le corps composé K_1K_2 sont corps de classes associés à H_1H_2 (groupe d'idéaux engendré par H_1, H_2) et $H_1 \cap H_2$, respectivement. Et on démontre de même sans difficulté le *théorème de translation*: Soient K le corps de classes sur k associé à H et k' une extension finie de k, H' le groupe d'idéaux de k' composé d'idéaux dont les normes à k tombent dans H. Alors le corps composé $K' = k'K$ est corps de classes sur k' associé à H'.

*

Takagi [3] démontre ensuite qu'une extension cyclique K/k de degré premier ℓ est un corps de classes. Il suffit de démontrer pour cela la deuxième inégalité pour une extension cyclique de degré ℓ. Cela se fait par un calcul assez compliqué des indices de divers groupes dont l'origine remonte à Gauss qui s'en est occupé dans ses Disquisitiones dans le cas où $k = \boldsymbol{Q}$, $\ell = 2$. (Hilbert a repris le même calcul dans [2] Chap.3, et on retrouve cette tradition continuée dans les calculs cohomologiques.)

Si en particulier ℓ est impair, le discriminant D de l'extension K/k se révèle être une $(\ell-1)$-ème puissance d'un idéal entier F de k, et on montre que le conducteur de H est un diviseur de F. Et quand k contient $\zeta = \exp(2\pi i/\ell)$, on sait d'après Kummer que $K = k(\sqrt[\ell]{\alpha})$, $\alpha \in k$, est le corps de classes associé à un groupe d'idéaux H dont on connait le conducteur en fonction de α. Takagi fixe un module M de k, et compte le nombre des extensions kummériennes $k(\sqrt[\ell]{\alpha})$ dont les conducteurs divisent M, et trouve que ce nombre est au moins égal au nombre des groupes d'idéaux d'indice ℓ dont les conducteurs divisent M. Ce fait assure l'existence du corps de classes de degré ℓ sur un corps k contenant ζ, et on voit avec un petit raisonnement supplémentaire que le conducteur de K/k est égal à F (*cf.* Iwasawa [4]).

Ainsi, dans le cas où le corps de base k contient une racine primitive ℓ-ième de l'unité ζ, on voit que pour tout groupe d'idéaux H d'indice ℓ, il existe un

et un seul corps de classes K de degré ℓ, tel que le groupe de Takagi $H(K)$ coïncide avec H donné. Et il est facile d'éliminer la condition "$\zeta \in k$" en vertu du Théorème de translation. Etant donnés le corps de base k quelconque et un nombre premier ℓ (pair ou impair), il s'établit donc qu'entre l'ensemble des extensions cycliques K de k de degré ℓ et celui des groupes d'idéaux H d'indice ℓ de k, il y a une bijection par la relation: K/k est corps de classes associé à H, et le groupe de Takagi $H(K)$ coïncide avec H.

Takagi développe ensuite la "théorie des genres" en vue de généraliser ce résultat pour les extensions cycliques de degré ℓ^ν, ν-ième puissance d'un nombre premier $\ell, \nu = 1,2,\ldots$. Nous n'entrerons pas dans la description de cette théorie qui n'est pas simple, parce qu'on peut l'éviter comme Herbrand a montré et arriver d'emblée au même résultat pour les extensions cycliques de degré quelconque (*cf.* Chevalley [2] Chap.I, IV), moyennant le fameux lemme de la théorie des groupes qui porte son nom. Puis le théorème de composition permet d'étendre ce résultat pour les extensions abéliennes en général parce celles-ci s'obtiennent par composition des extensions cycliques.

Après que Takagi a établi ainsi que toutes les extensions abéliennes sont corps de classes (d'après la "nouvelle définition"), il procède ainsi pour achever sa théorie.

Il commence par démontrer le *théorème d'existence*: Soit H un groupe d'idéaux dans le corps de base k. Il existe alors une extension K de k avec les propriétés: (1) K/k est une extension abélienne dont le groupe de Galois $G(K/k)$ est isomorphe au groupe quotient F/H, (2) Les ensembles des idéaux premiers qui divisent le conducteur de H et de ceux qui sont ramifiés dans K coïncident.

Nous avons déjà indiqué la démonstration de ce théorème pour le cas où l'indice $(F : H)$ de H est un nombre premier ℓ. On le généralise pour le cas $(F : H) = \ell^\nu, \nu = 1,2,\ldots$ par recurrence sur ν, puis pour le cas général par le théorème de composition. Comme K/k est une extension abélienne, c'est un corps de classes au sens de Takagi par le théorème d'unicité, pour lequel on peut utiliser le théorème de composition.

Enfin on démontre le *théorème de décomposition*: Soit K/k le corps de classes associé au groupe d'idéaux H. Un idéal premier P de k qui ne divise pas le conducteur de H appartient à une classe de F^E/H où E signifie l'ensemble des diviseurs premiers du conducteur de H. Alors le nombre minimal f tel que P^f tombe dans H coïncide avec le degré relatif de l'idéal premier $\bar{P}$ de K qui divise $P : N_{K/k}(\bar{P}) = P^f$. Il est en effet évident qui $N_{K/k}(\bar{P}) \in H$ d'après la définition même du groupe d'idéaux $H = H(K)$, donc $N_{K/k}(\bar{P}) = P^f$ implique $P^f \in H$, et on démontre la réciproque en réduisant au cas $f = 1$ en considérant le groupe de décomposition de $\bar{P}$ pour K/k.

La théorie du corps de classes étant ainsi essentiellement établie, Takagi l'appli-que dans le dernier Chap. de [3] au 12^{e} problème de Hilbert. Il est d'abord immédiat de voir que toute extension abélienne de $\boldsymbol{Q}$ est contenue

dans un corps circulaire $\boldsymbol{Q}(\zeta_m)$, parce que tout groupe d'idéaux dans $\boldsymbol{Q}$ contient le rayon $R_{mp_\infty} \bmod mp_\infty$. Une solution pour le cas où k est un corps quadratique imaginaire (où il s'agit donc de la théorie classique de la multiplication complexe) s'obtient aussi de la même manière, mais nous nous abstiendrons d'exposer ici les détails.

*

Au Congrès International des Mathématiciens à Strasbourg en 1920, Takagi a donné un exposé succinct de ces résultats et ajouté une question importante: Comment peut-on étendre cette théorie pour les extensions galoisiennes en général? Je crois que l'essai d'Artin (voir infra p.49) d'établir une théorie des fonctions zêta associées aux extensions galoisiennes qu'il a introduites dans [2] comme une nouvelle espèce de séries L et dont il a donné un exposé dans son mémoire [6], ainsi qu'une théorie des "conducteurs des extensions galoisienne" (*cf.* Artin [7]), indique une possibilité de traiter l'arithmétique des extensions galoisiennes (non-abéliennes en général) des corps de nombres algébriques en se basant sur la théorie du corps de classes, mais cela demeure une suggestion encore très vague. Il y a d'autre part des essais intéressants pour quelques cas spéciaux faits par Shimura [2] et développés par Ihara [1] de divers côtés, mais on est encore loin de pouvoir donner une réponse générale à cette question.

*

J'ai rapporté plus haut que Hilbert a posé comme le 9$^{\text{e}}$ problème au Congrès de Paris en 1900 la question de formuler et de démontrer la loi de réciprocité pour le reste de puissance en généralisant la loi de réciprocité quadratique de Gauss et que Furtwängler [1] y a donné une réponse en utilisant ses résultats sur la théorie du corps de classes au sens hilbertien. Rappelons que le symbole $\left(\frac{\mu}{A}\right)_m$ de reste de m-ième puissance est défini pour un entier $m \geq 2$, un élément μ et un idéal A satisfaisant à certaines conditions dans un corps de nombres algébriques de degré fini k qui contient $\zeta_m = \exp(2\pi i/m)$, de la manière suivante: il prend la valeur ζ_m^{ν}, $\nu \in \boldsymbol{Z}$ et on a $m|\nu$ si la congruence $\mu \equiv \xi^m \pmod{A}$ a une solution dans k. Un résultat classique d'Eisenstein [1], [2] dit qu'on a $\left(\frac{\mu_1}{(\mu_2)}\right)_m = \left(\frac{\mu_2}{(\mu_1)}\right)_m$ sous certaines conditions sur μ_1, μ_2. En possédant la théorie générale de corps de classes, Takagi [4] a rétabli, généralisé et simplifié les résultats de Furtwängler [1], et ajouté la remarque suivante: La valeur de $\left(\frac{\mu}{A}\right)_m$ dépend seulement de la classe de F^E/H à laquelle A appartient, où H est le groupe d'idéaux de k, auquel l'extension cyclique $k(\sqrt[m]{\mu})$ est associée, et E est l'ensemble des diviseurs premiers du conducteur de H. C'est cette remarque qui a suggéré à Artin l'idée de sa *loi générale de réciprocité* pour l'extension abélienne K/k.

*

Il me semble important de rappeler aussi que Artin a été conduit à cette idée de son essai d'entamer une théorie qui généraliserait la théorie du corps de classes pour les extensions galoisiennes. Dans son mémoire [2] en 1924, il a introduit une nouvelle espèce de séries L, généralisant les séries $L(s,\chi,H)$ définies plus haut (p.41)

$$L(s,\chi,H)=\sum_A^E \frac{\chi(A)}{N(A)^s}=\prod_P^E (1-\chi(P)N(P)^{-s})^{-1}$$

traitées par Hecke [3] et nommées souvent les *séries L de Hecke*, pour un groupe d'idéaux H dans un corps k et un caractère χ du groupe des classes $\Phi=F^E/H$. Par la théorie du corps de classes (que nous supposons ici achevée) il existe une extension abélienne K/k correspondant à H telle que $G(K/k)\cong\Phi$, et on peut noter $L(s,\chi,K/k)$ au lieu de $L(s,\chi,H)$. Artin a défini la série $L(s,\chi,K/k)$ pour une *extension galoisienne* K/k et pour un caractère du groupe $G(K/k)$ de sorte qu'elle coïncide avec celle de Hecke dans le cas où $G(K/k)$ est abélien. Il la définit comme suit: Comme $G(K/k)$ n'est pas abélien en général, on ne peut pas exprimer ses caractères par les racines de l'unité comme dans le cas abélien. Soit ρ une représentation de $G(K/k)$ dans le sens de Frobenius, c'est-à-dire un homomorphisme de $G(K/k)$ dans le groupe général linéaire de dimensions d sur $\boldsymbol{C}$: $GL(d,\boldsymbol{C})$. Un idéal premier P de k qui ne se ramifie pas dans K se décompose dans la forme $P=P_1\cdots P_g$ dans K et les automorphismes de Frobenius $\sigma_1,\ldots,\sigma_g$ de $P_1,\ldots,P_g$ sont conjugués dans $G(K/k)$. Les polynomes

$$\det(XE-\rho(\sigma_i)),\quad i=1,\ldots,g$$

se coïncident donc et ne dépendent que de P, et de la classe de conjugaison de ρ, dans $GL(d,\boldsymbol{C})$, qu'on peut noter χ. On pourra donc noter $A(P,\chi)$ au lieu de $\rho(\sigma_i)$. (C'est un élément de $GL(d,\boldsymbol{C})$.) Artin définit $L(s,\chi,K/k)$ par le produit eulérien:

$$L(s,\chi,K/k)=\prod_P^E \det(E-A(P,\chi)N(P)^{-s})^{-1}$$

où E indique l'ensemble des idéaux premiers de k qui se ramifient dans K. Si, en particulier, $\chi=\chi_0$ est le caractère principal, c'est-à-dire que ρ est la représentation identique de degré 1, on a

$$L(s,\chi_0,K/k)=\zeta_k(s)\prod_{P\in E}(1-N(P)^{-s}).$$

Ainsi $L(s,\chi_0,K/k)$ coïncide essentiellement avec la fonction zêta de Dedekind de k, et on voit que $L(s,\chi,K/k)$ coïncide avec la série de Hecke dans le cas où $G(K/k)$ est abélien, si la loi suivante est valable:

Soit K/k une extension abélienne associée au groupe d'idéaux H de k. Chaque classe de $\Phi = F^E/H$ contient un idéal premier P et l'automorphisme de Frobenius de P dépend seulement de cette classe. Si l'on fait correspondre à chaque classe de Φ cet automorphisme de Frobenius, on obtient un isomorphisme de Φ sur $G(K/k)$.

C'est cette loi qu'on appelle la *loi générale de réciprocité* d'Artin. La théorie de Takagi assure l'isomorphie $\Phi \cong G(K/k)$, mais cette loi la donne explicitement par l'intermédiaire de l'automorphisme de Frobenius.

Pour une extension abélienne K/k et un idéal premier P de k qui ne se ramifie pas dans K, Hasse [2] a noté $\left(\frac{K/k}{P}\right)$ l'automorphisme de Frobenius de P. En outre, pour un idéal $A = P_1^{e_1} \cdots P_r^{e_r}$ de k avec $P_1, \ldots, P_r \notin E$, il a noté

$$\left(\frac{K/k}{A}\right) = \left(\frac{K/k}{P_1}\right)^{e_1} \cdots \left(\frac{K/k}{P_r}\right)^{e_r}$$

et l'a appelé le *symbole d'Artin*. (Quand k est fixé, on peut simplifier $\left(\frac{K/k}{A}\right)$ par $\left(\frac{K}{A}\right)$.) La remarque de Takagi dit que $\left(\frac{K}{A}\right)$ ne dépend que de la classe de Φ à laquelle A appartient, et la loi d'Artin dit que l'application: classe de $A \to \left(\frac{K}{A}\right)$ effectue l'isomorphisme de Φ avec $G(K/k)$. Et pour le cas spécial $k \ni \zeta_m$, $K = k(\sqrt[m]{\mu})$, le symbole de reste de m-ième puissance $\left(\frac{\mu}{A}\right)_m$ s'interprète pour $\left(\frac{K/k}{A}\right) \sqrt[m]{\mu} \Big/ \sqrt[m]{\mu}$!

On voit ainsi que cette loi couvre les théorèmes d'isomorphie et de décomposition de la théorie du corps de classes de sorte qu'il suffirait de la démontrer avec le théorème d'existence pour la rétablir complètement. Mais Artin n'a pas pu le démontrer tout de suite. Il a montré seulement qu'elle est valable dans plusieurs cas simples (en particulier pour le cas où K/k est une extension circulaire) et l'a présenté comme une conjecture qu'il est arrivé à démontrer quatre ans plus tard dans [3].

*

La loi d'Artin qu'on peut regarder comme la clef de voûte de notre théorie, concrétise ainsi le théorème d'isomorphie et précise le théorème de décomposition. On est tenté de la démontrer en utilisant et précisant la démonstration de ces derniers théorèmes, mais cela ne marche pas. D'autre part, on voit facilement que cette loi est valide pour les extensions circulaires. Artin a réussi à la

démontrer en utilisant la méthode dite du *croisement avec une extension circulaire*. Sans entrer dans les détails techniques, nous allons en donner une esquisse historique.

*

Soient K/k une extension galoisienne, P un idéal premier de K qui n'est pas ramifié dans K/k et $\overline{P}$ un idéal premier de K contenant P. L'importance de l'élément de $G(K/k)$, qu'on appelle maintenant l'*automorphisme de Frobenius* pour $\overline{P}$, a été relevé par Frobenius [1], où il a émis la conjecture suivante: Soit C une classe de conjugaison de $G(K/k)$, c'est-à-dire $C = C(g_0) = \{g \in G(K/k); g = hg_0h^{-1}, h \in G(\underline{K}/k)\}$ pour un élément g_0 de $G(K/k)$. Si l'automorphisme de Frobenius de P appartient à C, on dira pour simplifier que P appartient à C, parce que cette classe ne dépend que de P. La conjecture de Frobenius dit que la densité (au sens de p.44) de l'ensemble des idéaux premiers de k qui appartiennent à C est $|C|/|G(K/k)|$. Frobenius a montré qu'elle est valide dans plusieurs cas spéciaux dont on peut tirer de belles conséquences.

C'est Tschebotareff [1] qui a démontré cette conjecture, en remarquant d'abord qu'elle est vraie pour les extensions circulaires, et en montrant ensuite qu'on peut la démontrer dans le cas général en construisant une extension circulaire adaptée à la situation et en la "croisant" avec l'extension donnée. Schreier [1] a dégagé cette méthode dans le mémoire de Tschebotareff, dont Artin a reconnu la grande utilité, et a réussi en l'employant à établir sa loi. Tout de suite après la parution du mémoire d'Artin [3], Takagi a fait un article en japonais [5] où il a exprimé son admiration pour ce beau résultat.

Bien que la nature de cette méthode de croisement soit essentiellement arithmétique, la démonstration d'Artin [3] repose sur le théorème de décomposition, démontré par Takagi par méthode analytique, et il faut rappeler aussi que la loi d'Artin avait été suggérée par les nouvelles séries L, entités analytiques en vue de répondre au problème de Takagi pour généraliser la théorie du corps de classes aux extensions galoisiennes non-abéliennes.

*

En 1931–32, Chevalley ayant terminé ses services militaires, a obtenu une subvention pour faire séjour à Hambourg où Artin a donné un cours sur la théorie du corps de classes avec la nouvelle démonstration, et les simplifications apportées par Herbrand, Chevalley ainsi que par Artin lui-même. La définition du corps de classes y a été donnée d'après Takagi, d'où les théorèmes d'ordre, d'unicité etc. découlent comme nous avons remarqué plus haut (p.47). Le lemme d'Herbrand a dispensé la théorie des genres de Takagi et la démonstration du théorème d'existence a été présenté en forme simplifiée par Herbrand et Chevalley (Herbrand [2]). Ensuite, les théorèmes du conducteur et de décomposition et

enfin la loi d'Artin ont été démontrés d'après les méthodes découvertes quelques années d'avant.

J'ai eu la chance de suivre ce cours d'Artin à Hambourg en même temps que Chevalley. En l'écoutant, Chevalley a souvent eu l'idée pour améliorer la présentation qu'il m'a tout de suite communiqué ainsi qu'à Artin, dont celui-ci a fait part aux auditeurs au début de l'heure suivante chaque fois qu'il l'a trouvée intéressante. C'est pendant cette période que Chevalley a repensé sur la structure générale de cette théorie et a eu l'idée de la réorganiser sur les axes de deux concepts: celui du groupe de Takagi et celui du groupe d'Artin. Il l'a publié dans sa note de CR [1], puis dans sa Thèse [2] dans tous les détails. (Une fois, il a même pensé qu'il aurait pu arithmétiser ainsi toute cette théorie, mais il s'est aperçu tout de suite de ses erreurs: Tout pourrait être arithmétisé, si l'on pouvait démontrer sans méthode analytique que les extensions circulaires sont corps de classes. Or, on avait alors encore besoin d'utiliser la méthode d'analyse pour établir ce point. Comme nous l'avons déjà dit, l'arithmétisation complète a été atteinte dans ses travaux ultérieurs [3], [6].)

*

Comme ce volume[3] contient le texte intégral de la Thèse [2], ce serait inutile d'en répéter le contenu et je pourrai me borner à en esquisser les grandes lignes et en relever quelques points importants.

Ce mémoire [2] présuppose la connaissance de la partie élémentaire de la théorie algébrique des nombres telle que nous avons expliqué plus haut, mais expose la théorie entière du corps de classes, la loi d'Artin y comprise, avec toutes les démonstrations détaillées. Chevalley y évite autant que possible les méthodes analytiques, qui ne sont utilisées que pour démontrer que les corps circulaires sont corps de classes (Chap.VII).

Chevalley commence cette Thèse par donner dans son Introduction un aperçu historique de cette théorie, dont on trouve une récapitulation à la fin (Chap.X). Tous les résultats de Takagi [3], et Artin [3] se retrouvent ici (sauf, bien entendu, l'existence d'une infinité d'idéaux premiers dans chaque classe de F^E/H dans notre notation habituelle.)

*

Ainsi Chevalley a eu l'idée d'attacher l'importance à ce qu'il a nommé le *groupe d'Artin* et le *groupe de Takagi* définis comme suit: K/k étant une extension galoisienne, nous avons déjà parlé du groupe de Takagi $H(K) = H(K/k)$, (et vu comment Takagi a défini son corps de classes par la coïncidence de son indice avec le degré d'extension.) D'autre part, nous avons vu que Hasse a défini le

[3] see $\star$.

symbole d'Artin $\left(\frac{K/k}{A}\right) = \left(\frac{K}{A}\right)$ pour une extension abélienne K/k et $A \in F^E$ comme un produit d'automorphismes de Frobenius

$$\left(\frac{K}{A}\right) = \prod_{i=1}^{r} \left(\frac{K}{P_i}\right)^{\nu_i} \quad \text{si} \quad A = \prod_{i=1}^{r} P_i^{\nu_i}.$$

Il est clair d'après cette définition qu'on a

$$\left(\frac{K}{AB^{-1}}\right) = \left(\frac{K}{A}\right)\left(\frac{K}{B}\right)^{-1} \quad \text{pour} \quad A, B \in F^E,$$

de sorte que le sousensemble $\left\{A \in F^E; \left(\frac{K}{A}\right) = 1\right\}$ forme évidemment un sous-groupe de F^E, (E étant comme d'habitude l'ensemble des idéaux premiers de k qui se ramifient dans K.) C'est ce sousgroupe que Chevalley appelle le *groupe d'Artin* pour K/k. Désignons-le par $H_0 = H_0(K/k)$. La loi d'Artin s'exprime alors par $H(K/k) = H_0(K/k)$. C'était le groupe de Takagi $H(K/k)$ qui a joué le rôle principal dans la théorie de Takagi. Chevalley a conçu l'idée de la reconstruire en commençant par considérer le groupe d'Artin $H_0(K/k)$. Le résultat fondamental de Takagi-Artin, que chaque extension abélienne K/k est corps de classes, pour lequel la loi d'Artin s'applique, a été reformulé par Chevalley en deux théorèmes suivants:

Théorème A. K/k étant une extension abélienne, soient E l'ensemble des idéaux premiers de k qui se ramifient dans K et F^E le groupe des idéaux (non nuls) de k qui sont premiers aux éléments de E. Alors F^E a un sousgroupe H_0 avec les deux propriétés: 1) Si P est un idéal premier $\notin E$, et $\overline{P}$ un diviseur premier de P dans K, on a $N_{K/k}(\overline{P}) = P^f$, où f est l'exposant minimal tel que $P^f \in H_0$; 2) Le groupe quotient F^E/H_0 est isomorphe à $G(K/k)$.

Théorème B. Il existe un module M_0 de k composé d'idéaux premiers de E et des places de k qui se ramifient dans K, avec les deux propriétés: 1) $H_0 \supset R_{M_0}$ (c'est-à-dire que le groupe H_0 mentionné dans le théorème A contient le rayon mod M_0, de sorte que H_0 peut être pris comme un groupe d'idéaux définissable mod M_0); 2) M étant un module quelconque de k tel que $M_0|M$, le groupe $H_0(M)$ des idéaux de H_0 qui sont relativement premiers à M coïncide avec le groupe de Takagi $H(K/k, M)$ (c'est-à-dire le sousgroupe de $F^{E(M)}$ engendré par le rayon R_M et les normes de K/k des idéaux de K relativement premiers à M.)

En fait, on démontre d'abord le Théorème A, en faisant voir que le groupe d'Artin H_0 défini plus haut ont des propriétés 1), 2) de ce Théorème, et puis on démontre le Théorème B en utilisant la méthode de croisement. (Chap.VIII)

La démonstration du Théorème A est donnée dans le même Chap.VI où ces Théorèmes sont formulés. Il est évident que le groupe d'Artin H_0 a la propriété

1) de sorte qu'il suffit de montrer $F^E/H_0 \cong G(K/k)$, ce qui équivaut à dire que le symbole d'Artin $\left(\frac{K/k}{A}\right)$ prend tout élément de $G(K/k)$ comme valeur.

Le symbole d'Artin a d'autre part les propriétés suivantes qui découlent tout de suite de sa définition: 1) Si $k \subset K' \subset K$, l'automorphisme $\left(\frac{K'}{A}\right) \in G(K'/k)$ n'est autre chose que la restriction de l'automorphisme $\left(\frac{K}{A}\right) \in G(K/k)$ sur K', ce qu'on exprime par $\left(\frac{K}{A}\right) \to \left(\frac{K'}{A}\right)$; 2) Si $K = K_1K_2$ (corps composé) et $k = K_1 \cap K_2$ on a $\left(\frac{K/k}{A}\right) = \left(\frac{K_1}{A}\right)\left(\frac{K_2}{A}\right)$, et 3) Si $k \subset K$, $k \subset k'$ et A' est un idéal de k' composé d'idéaux premiers qui ne se ramifient pas dans Kk', on a $\left(\frac{Kk'/k'}{A'}\right) = \left(\frac{K/k}{N_{k'/k}(A')}\right)$. A ces trois propriétés du symbole d'Artin correspondent les trois propriétés du groupe d'Artin: 1) Si $K' \subset K$, on a $H_0(K') \supset H_0(K)$, 2) Si $K = K_1K_2$, on a $H_0(K) = H_0(K_1) \cap H_0(K_2)$; 3) Si $K' = Kk', H_0(K'/k')$ est le sousgroupe des idéaux de k' qui ne se ramifient pas dans K' dont les normes à k tombent dans $H_0(K/k)$. Grâce à ces résultats, la constatation du fait que le symbole $\left(\frac{K}{A}\right)$ prend toutes les valeurs de $G(K/k)$ se ramène au cas où $G(K/k)$ est un groupe cyclique de degré qui est puissance d'un nombre premier, en vertu du théorème fondamental sur les groupes abéliens finis.

Chevalley s'est aperçu que ce dernier fait s'ensuit de la "deuxième inégalité" $n \leq h$ où $n = (K : k)$, $h = (F^E : H)$, H étant le groupe de Takagi $H(K/k)$. Comme nous l'avons déjà dit, cette inégalité (pour les extensions cycliques) se démontre arithmétiquement (avec un calcul assez compliqué). Cette démonstration est donnée dans le Chap.VIII avec le corollaire qu'il doit y avoir un idéal premier P de k qui reste premier dans K quand K/k est une extension cyclique de degré qui est puissance d'un nombre premier. Pour un tel idéal premier P, $\left(\frac{K}{P}\right)$ doit engendrer le groupe $G(K/k)$, de sorte que l'ensemble de valeur de $\left(\frac{K}{A}\right)$ remplit tout le groupe $G(K/k)$.

En citant ce résultat démontré ultérieurement, Chevalley achève la démonstration du Théorème A dans le Chap.VI.

Dans le Chap.VII sur les corps circulaires qui en fait la suite, Chevalley démontre moyennant ici la méthode analytique (malgré lui sans doute) que les corps circulaires sont corps de classes, c'est-à-dire que si $K = k(\zeta_m)$, $\zeta_m = \exp(2\pi i/m)$, m étant un entier positif, le groupe d'Artin $H_0(K/k)$ coïncide avec le groupe de Takagi $H(K/k)$ qui est définissable $\bmod mp_\infty$. Comme il est facile de montrer $H_0(K/k) \supset R_{mp_\infty}$, et par suite $H_0(K/k) \supset H(K/k)$, et d'autre part

on a $h = (F^E : H(K/k)) \leq n = (K : k) = (F^E : H_0(K/k))$ (la dernière égalité grâce au Théorème A) par la considération analytique (la "première inégalité"), on obtient tout de suite le résultat.

Ce Chap.VII contient un "théorème d'existence" d'un certain nombre premier dont on a besoin quand on utilise la méthode de croisement pour démontrer le Théorème B dans le Chap.VIII. Je me permets de faire remarquer ici qu'on atteint le même but en remplaçant le nombre premier par la puissances d'un nombre premier ce qui simplifie considérablement la démonstration.

Plus présicément, il s'agit du théorème suivant d'arithmétique élémentaire: Etant donnés des entiers n, a quelconques, $n \geq 2$, $a \geq 2$, il existe une infinité de nombres premiers q tels que le plus petit exposant f pour lequel $a^f \equiv 1 \pmod{q}$ (c'est-à-dire l'ordre de a dans $(\boldsymbol{Z}/q\boldsymbol{Z})^\times$) soit divisible par n. On se sert de ce théorème dans la démonstration du Théorème B pour le cas où K/k est cyclique pour construire une extension circulaire et cyclique K'/k telle que $K' \cap K = k$ et que l'ordre de $\left(\frac{K'}{P}\right)$ pour un idéal premier P donné d'avance dans k soit divisible par $n = [K : k]$. Il suffira de poser $K' = k(\zeta_q)$, q étant un nombre premier approprié dont l'existence est assuré par ce "théorème d'existence." Or, si l'on remplace la condition que "q soit un nombre premier" par "q soit une puissance d'un nombre premier impair", l'extension $k(\zeta_q)/k$ sera toujours circulaire et cyclique, et cela ne causera aucun inconvénient à l'usage dans la dite démonstration du Théorème B. Et si l'on adoucit ainsi la condition pour q, la démonstration du théorème élémentaire pourra se faire simplement comme suit. (*cf.* Iyanaga [1], [4])

Soit $\Phi_n(X) = \prod(X - \zeta_i)$, ζ_i étant les racines primitives n-ièmes de l'unité, le polynôme dit *cyclotomique* d'ordre n, dont le degré est $\varphi(n)$. Comme $n \geq 2$, $a \geq 2$, on a $|\Phi_n(a)| = \prod|a - \zeta_i| > 1$, donc $\Phi_n(a) \neq \pm 1$. Soit ℓ un nombre premier diviseur de $\Phi_n(a)$. Remarquons que $\Phi_n(X)$ est un diviseur de $X^n - 1 = \prod_{j=0}^{n-1}(X - \zeta^j)$ avec $\zeta = \exp(2\pi i/n)$ dans $\boldsymbol{Z}[X]$. Il y a donc un $\Psi_n(X) \in \boldsymbol{Z}[X]$ avec $X^n - 1 = \Phi_n(X)\Psi_n(X)$. On a ainsi $\ell \,|\, \Phi_n(a) \,|\, (a^n - 1)$. Supposons $\ell^\mu \parallel (a^n - 1)$, c'est-à-dire que $\ell^\mu \,|\, (a^n - 1)$, $\ell^{\mu+1} \not| (a^n - 1)$, et posons $q = \ell^\mu$. On a alors $a^n \equiv 1 \pmod{q}$. On va voir que n est exactement l'ordre de a dans $(\boldsymbol{Z}/q\boldsymbol{Z})^\times$. Soit n_0 cet ordre de a. Si l'on avait $n_0 < n$, on aurait $n_0 \,|\, n$, $q \,|\, (a^{n_0} - 1)$, mais $X^{n_0} - 1$ avec $n_0 < n$, $n_0 \,|\, n$ serait un diviseur de $X^n - 1$ dans $\boldsymbol{Z}[X]$ qui n'a pas de facteur commun avec $\Phi_n(X)$, donc diviseur de $\Psi_n(X)$, d'où $q \,|\, \Psi_n(a)$, ce qui serait en contradiction avec $\ell^\mu \parallel (a^n - 1) = \Phi_n(a)\Psi_n(a)$ parce que $\ell \,|\, \Phi_n(a)$. En remplaçant n par $n' = np$, p étant un nombre premier $> \ell$, on verra qu'il y a un autre $q' = \ell'^{\mu'}$ tel que l'ordre de a dans $(\boldsymbol{Z}/q\boldsymbol{Z})^\times$ soit n' qui est divisible par n. On aura $\ell' \neq \ell$ parce que $p \,|\, n' \,|\, \varphi(q') = \ell'^{\mu'-1}(\ell' - 1)$, d'où $\ell < p < \ell'$. Ainsi on a une infinité de puissances de nombres premiers distincts $q, q', \ldots$ de sorte que l'ordre de a dans $(\boldsymbol{Z}/q\boldsymbol{Z})^\times$, $(\boldsymbol{Z}/q'\boldsymbol{Z})^\times$ soit divisible par n. (En particulier, on peut trouver un q impair.)

*

Le Chap.VIII qui contient la démonstration du Théorème B constitue certainement la partie culminante de cette Thèse. Il commence par la première partie reprenant la vieille théorie de Gauss sur les formes quadratiques, généralisée par Takagi pour les extensions cycliques de degrés puissances de nombres premiers. On voit cette théorie exposée ici d'emblée pour les extensions cycliques de degrés quelconques, ce qui est devenu possible grâce au lemme d'Herbrand de la théorie des groupes. La "deuxième inégalité" est démontrée ainsi pour les extensions cycliques. Chevalley démontre ensuite le Théorème B pour les extensions cycliques par la méthode de croisement en utilisant le "théorème d'existence" qui vient d'être démontré dans le Chap. précédent. Je m'abstiendrai de répéter ici l'argument très ingénieux de Chevalley clairement exposé dans le texte.

La généralisation pour les extensions abéliennes quelconques n'offre plus de difficulté. Le Chapitre se termine par le "théorème du genre principal." et le "théorème de Hasse" sur les extensions cycliques et la remarque que le théorème de Kronecker affirmant que toutes les extensions abéliennes de $\boldsymbol{Q}$ sont contenues dans un corps circulaire est un corollaire immédiat de notre théorie.

*

Le Chap.IX est consacré à la théorie du corps de classes local. Dans la théorie du corps de classes dont nous avons parlé jusqu'ici, toutes les places du corps de base k sont tenues en considération tandis que dans la théorie dont on s'occupe dans ce Chap.IX, on considère comme corps de base un corps local, c'est-à-dire la complétion k_P de k à une place déterminée P, d'ailleurs non-archimédienne. Il s'agit de la théorie des extensions abéliennes de k_P. Pour distinguer, on appelle la théorie jusqu'ici considérée la *théorie globale* par opposition à la *théorie locale* traité dans ce Chapitre. Cette dernière est plus simple que la théorie globale, mais historiquement on l'avait déduite comme corollaire de celle-ci. (Hasse [4], F. K. Schmidt [1]). Chevalley l'a fondée ici pour la première fois indépendamment de la théorie globale, et par les moyens purement arithmétiques.

Soit k un corps local, c'est-à-dire k_P dans la vieille notation. (Pendant que nous parlerons du contenu du Chap.IX, nous abandonnerons cette vieille notation. De même K, K' etc. signifiront les corps locaux.)

Pour une extension finie K/k, on définie comme d'habitude la norme $N_{K/k}(\bar{\alpha}) \in k$ pour tout élément $\bar{\alpha} \in K$; alors le sousensemble $\{N_{K/k}(\bar{\alpha}); \bar{\alpha} \in K^\times\}$ de $k^\times$ forme évidemment un sousgroupe de $k^\times$. On appelle ceci le sousgroupe de $k^\times$ *associé à* K et le notera $H(K/k)$ (en analogie avec le groupe de Takagi dans la théorie globale.) Le résultat de la théorie locale peut alors s'exprimer aisni:

Soient K/k une extension quelconque de corps local de degré fini $n = [K : k]$ et $H = H(K/k)$ le sousgroupe de $k^\times$ associé à K/k. Alors H a toujours un indice $h = (k^\times : H)$ fini dans $k^\times$, $h \leq n$ et on a $h = n$ si et seulement si K/k est abélien. (Dans le cas général, on a $H(K/k) = H(K'/k)$, où K' est le corps intermédiaire $k \subset K' \subset K$ maximal de K/k de sorte que K'/k soit abélien.) Quand on a $(K : k) = n = h = (k^\times : H)$, on dit que K est le *corps de classes pour* H. On voit que les deux faits: (i) K/k est abélien et (ii) K est le corps de classes pour $H = H(K/k)$ sont équivalents. Et on démontre que si K_1, K_2 sont les corps de classes pour H_1, H_2 respectivement, $K_1 \subset K_2$ et $H_1 \supset H_2$ s'entraînent mutuellement (*théorème de comparaison*) et en particulier il n'y a qu'un seul corps de classes pour un sousgroupe donné de $k^\times$ (*théorème d'unicité*). De plus, pour chaque sousgroupe H d'indice fini de $k^\times$, il existe un corps de classes K pour H (*théorème d'existence*). Bref, tous les théorèmes de la théorie globale trouvent leurs homologues dans la théorie locale dans une forme simplifiée.

On s'est aperçu plus tard que le traitement cohomologique convient particulièrement pour l'exposition de cette théorie comme Serre [1] l'a magistralement montré, et d'un autre côté celle-ci s'exprime aussi dans le cadre de la théorie des groupes formels, comme Hazewinkel [1] l'a fait voir. Iwasawa a donné deux versions [2], [3], également merveilleuses de cette théorie où il en a montré en particulier les applications aux belles formules explicites de loi de réciprocité. Elle est liée aussi à la théorie du groupe de Brauer des classes d'algèbres, et Chevalley a eu l'idée de construire la théorie globale à partir de la théorie locale, en utilisant la théorie des algèbres. Il l'a communiqué à Weil, qui a exposé la théorie du corps de classes dans son livre [12] basée sur cette idée de Chevalley et non pas sur la théorie cohomologique, comme c'était en mode dans les 1960, époque de la publication de ce livre.

*

La Thèse s'achève avec le Chap.X où les théorèmes d'existence et de conducteur sont démontrés. Nous avons déjà dit que Chevalley avait commencé ses publications arithmétiques par sa note en collaboration avec Herbrand [2] sur la démonstration du théorème d'existence, travail qui avait été le premier pas vers l'arithmétisation de la théorie du corps de classes. En fait, la vieille démonstration s'appuyait sur l'existence d'une infinité des idéaux premiers dans chaque classe de F^E/H, H étant un groupe d'idéaux donné, mais Herbrand et Chevalley ont pu éviter d'utiliser ce résultat analytique en concevant ce qu'ils ont appelé "les modules complémentaires," dont nous parlerons tout à l'heure.

Le théorème d'existence dit que, étant donné un corps de nombres algébriques de degré fini k et un groupe d'idéaux H dans k, il existe une extension abélienne K/k de sorte que le groupe de Takagi $H(K/k)$ coïncide avec H.

Pour simplifier notre exposé, écrivons provisoirement $K/k \leftrightarrow H$ pour signifier que K/k est l'extension abélienne pour laquelle $H(K/k) = H$, c'est-à-

dire que K est le corps de classes sur k associé à H. D'après ce que nous savons déjà sur les relations entre K/k et H, on peut facilement voir par exemple que si $K/k \leftrightarrow H$, et $F^E \supset H' \supset H$, il y a un (et un seul) corps intermédiaire K' tel que $k \subset K' \subset K$ de sorte que $K'/k \leftrightarrow H'$, et si $K_1/k \leftrightarrow H_1$, $K_2/k \leftrightarrow H_2$, on a $(K_1 \cap K_2)/k \leftrightarrow H_1 H_2$ (le groupe d'idéaux engendré par H_1, H_2) et $K_1 K_2/k \leftrightarrow H_1 \cap H_2$, ($K_1 K_2$ est le corps composé de K_1, K_2), d'où s'ensuit qu'il suffit de démontrer le théorème d'existence pour H pour lequel F^E/H est cyclique d'ordre n qui est une puissance d'un nombre premier. (Chevalley et Herbrand l'ont démontré d'emblée pour le cas où F^E/H est cyclique d'ordre quelconque n.)

On peut réduire cette démonstration au cas où le corps de base k contient une racine primitive n-ième de l'unité ζ, en vertu du lemme suivant qu'on obtient facilement comme une application de la théorie de Galois: Soient $K \supset k_1 \supset k$, K/k_1 abélien, $K/k_1 \leftrightarrow H_1$ celui-ci étant un groupe d'idéaux dans k_1, et k_1/k cyclique. Si l'on a $\tau(A_1 H_1) = A_1 H_1$ pour tous les idéaux A_1 de $F_1^{E_1}$ de k_1 et pour tous les éléments τ de $G(k_1/k)$, K/k est abélien.

Pour construire une extension K/k pour H donné pour lequel F^E/H et cyclique d'ordre n, on adjoint d'abord une racine primitive n-ième ζ à k, pose $k_1 = k(\zeta)$ et $H_1 =$ le groupe d'idéaux dans k_1 dont les normes à k tombent dans H. L'extension K_1 de k_1 pour lequel $K_1/k_1 \leftrightarrow H_1$ donne l'extension cherchée $K/k \leftrightarrow H, K_1 = Kk_1$.

Supposons donc que le corps de base k contient une racine primitive n-ième de l'unité ζ. Toute extension cyclique de k de degré n s'obtient alors par l'adjonction d'une racine n-ième d'un élément $a \in k : K = k(\sqrt[n]{\alpha})$, comme Chevalley l'a montré dans le Chap.IV comme un corollaire du théorème normique de Hilbert, disant que tout élément A de l'extension cyclique K de k avec $G(K/k) = \{1, \sigma, \ldots, \sigma^{n-1}\}$ pour lequel $N_{K/k}(A) = 1$, peut se mettre sous la forme $A = B^{1-\sigma}$, avec $B \in K$. (Rappelons-nous qu'on appelle depuis le *Zahlbericht* de Hilbert une *extension kummérienne* d'un corps k contenant une racine primitive n-ième de l'unité ζ toute extension K de la forme $k(\sqrt[n]{\alpha})$, $\alpha \in k$, car Kummer l'avait étudié dans ses recherches du problème de Fermat.)

Considérons maintenant n comme un entier ≥ 2 fixé pour le moment. Soient k un corps contenant une racine primitive n-ième de l'unité ζ, P une place de k finie ou infini de k et $\alpha \in k$. Chevalley appelle α *primaire* pour P si P ne se ramifie pas dans $k(\sqrt[n]{\alpha})$ et *hyperprimaire* pour P si P se décompose complètement dans $k(\sqrt[n]{\alpha})$. Pour P infinie, ces concepts n'ont point d'intérêt que si $n = 2$, et dans ce cas ils s'identifient. Dans la suite, nous ne considérons qu'exceptionnellement que les places finies, dans lequel cas P peut être regardé comme un idéal premier de k.

Soient donc P une place finie ou un idéal premier de k. La complétion de k à cette place, c'est-à-dire le corps P-adique sur k se notera k_P. On voit facilement que la condition pour α, d'être hyperprimaire pour P équivaut à $k_P(\sqrt[n]{\alpha}) = k_P$

et qu'il y a un nombre critique c pour α pour lequel $\alpha \equiv 1 \pmod{P^\nu}$ avec $\nu \geq c$ garantie l'hyperprimarité de α pour P tandis que $\alpha \equiv 1 \pmod{P^\mu}$ avec $\mu < c$ ne le garantie pas. Le module P^c avec cet exposant critique s'appelle d'après Chevalley le *module d'hyperprimarité* pour P. En ce qui concerne la *primarité* de α pour P, on voit qu'il est nécessaire pour α pour être primaire pour P que son ordre pour α soit multiple de n, et si P n'est pas un diviseur de n, cette condition est suffisante aussi.

Les deux modules M_1, M_2 de k sont dits *complémentaires* s'ils satisfont à trois conditions suivantes: 1) $(M_1, M_2) = 1$, 2) Pour tout idéal premier P divisant $M_i (i = 1,2)$, M_i est divisible aussi par le module d'hyperprimarité pour P, 3) Tout idéal premier divisant n et toute place infinie divise l'un d'eux. Remarquons que si l'on se donne un des M_1, M_2 satisfaisant à ces conditions, on peut toujours en trouver l'autre (d'une manière qui n'est généralement pas unique.)

On associe à deux modules complémentaires M_1, M_2 de k deux groupes d'idéaux H_1, H_2 et deux extensions abéliennes K_1, K_2 de k définis comme suit. On notera E_1, E_2 les ensembles des places qui divisent M_1, M_2 respectivement. (On a $E_1 \cap E_2 = \emptyset$ à cause de 1) et $E_1 \cup E_2$ contient l'ensemble des places divisant n et des places infinies de k selon 3)). (1) H_1 est contenu dans F^{E_1} et engendré par $(F^{E_1})^n$, le rayon R_{M_1} et les idéaux premiers de E_2, (1′) H_2 se définit comme H_1 en permutant les indices 1, 2, (2) K_1 est le corps composé de toutes les extensions kummériennes $k(\sqrt[n]{\omega})$ de k, où ω parcourt tous les nombres de $k^\times$ qui sont primaires pour tout idéal premier ne divisant pas M_1, premiers à M_2 et hyperprimaires pour tout idéal premier diviseur de M_1; (2′) K_2 s'obtient de K_1 par permutation de 1, 2 dans sa définition.

De cette définition se découle le fait que le groupe de Takagi $\bmod M_1$ de $K_1/k : H(K_1/k, M_1)$ contient H_1 et de même $H(K_2/k, M_2) \supset H_2$. On aura donc $(F^{E_i} : H_i) \geq (F^{E_i} : H(K_i/k, M_i)) = (K_i : k)$, la dernière égalité selon le résultat déjà obtenu de la théorie des corps de classes $(i = 1,2)$. Par un calcul d'indices assez compliqué, on démontre l'égalité $(F^{E_1} : H_1)(F^{E_2} : H_2) = (K_1 : k)(K_2 : k)$, d'où l'on obtient $K_i \leftrightarrow H_i$, $i = 1,2$. Ainsi on voit que les corps de classes K_1, K_2 existent pour les groupes d'idéaux H_1, H_2 associés à une paire de modules complémentaires.

Reste à montrer qu'on peut trouver deux modules complémentaires M_1, M_2 de sorte qu'un des groupes d'idéaux associés H_1, H_2 soit contenu dans un groupe d'idéaux donné H, sur lequel on peut supposer que F^E/H soit cyclique d'ordre n, E étant l'ensemble des places divisant le conducteur de H. Pour ce faire, on prend un idéal premier quelconque Q dans H et pose $M_2 =$ (le module d'hyperprimarité pour Q), $M_1 =$ (un module complémentaire à M_2) et constate facilement que H_1 est contenu dans H. Le théorème d'existence s'établit ainsi.

Chevalley termine sa Thèse en démontrant le théorème du conducteur, affirmant que les diviseurs premiers, finis ou infinis, du conducteur du corps de

classes K sont ceux qui se ramifient dans K. Il le démontre d'abord pour le cas où $(K:k)$ est un nombre premier, auquel cas le cas général est réduit par récurrence sur $(K:k)$.

J'ajouterai que cette Thèse a été rédigée pendant les vacances d'été 1932, juste avant le Congrès International des Mathématiciens à Zurich, où Takagi est venu assister. Chevalley a participé aussi à ce Congrès où il a fait la connaissance personnelle de Takagi. Il lui a remis une copie de sa Thèse qui a été publiée dans le "Journal of the Faculty of Science" de Tokyo en 1933, dans le même journal où le mémoire de Takagi [6] avait paru en 1920.

*

L'idée d'achever la démonstration purement arithmétique de la théorie du corps de classes était sûrement un sujet de préoccupation de Chevalley même après la soutenance de sa Thèse. Un des étudiants qui suivaient le cours d'Artin à Hambourg en même temps que nous, Nehrkorn, à qui Chevalley avait communiqué les résultats de sa Thèse, a fait alors remarquer que le mémoire récent [5] de Hasse sur la théorie des algèbres contient une formule exprimant la loi d'Artin, qui servirait à démontrer arithmétiquement le Théorème B de sa Thèse. Chevalley a pu le confirmer et publié ce résultat dans une note [3] en collaboration avec Nehrkorn. Ainsi on a eu la première démonstration arithmétique de notre théorie en 1935, mais comme cette note ne me paraît pas appartenir au courant principal du développement d'idée de Chevalley, j'en parlerai tout à la fin de cet article (*cf.* infra p.78). Vers la même époque, il a découvert que cette théorie se formule et se généralise dans une forme beaucoup plus élégante en introduisant une nouvelle notion, qu'il a appelé "élément idéal", mais qu'on appelle maintenant "idèle" d'après une suggestion de Hasse. Cette idée a été présentée dans son mémoire "Généralisation de la théorie du corps de classes pour les extensions infinies" [5].

*

Soit k un corps de nombres algébriques de degré fini $n = r_1 + 2r_2$ avec r_1 conjugués réels et $2r_2$ conjugués complexes. On a vu que k possède alors $r_1 + r_2$ places archimédiennes dont r_1 réelles et r_2 complexes, et une infinité de places non-archimédiennes, dont chacune correspond à un idéal premier P de k. A chaque place v correspond un corps local k_v; selon que v est réelle, complexe ou non-archimédienne correspondant à P, k_v s'identifie avec $\boldsymbol{R}, \boldsymbol{C}$ ou le corps P-adique k_P. On se rappelle qu'on a noté $e_P(a) = v \in \boldsymbol{Z}$ pour $a \in k^\times$ si $P^v \parallel (a)$. Si $\alpha \in k_P$, il y a une suite d'éléments $a_1, a_2, \ldots \in k$ qui covergent vers α. Si $e_P(a_1), e_P(a_2), \ldots \to \infty$, on a évidemment $\alpha = 0$; sinon cette suite des entiers finissent par avoir la même valeur qui définit la valeur de $e_P(\alpha)$. Si $e_P(\alpha) = 0, \alpha$ se dit une *unité* de k_P, dont l'ensemble est noté U_P. Si v est

archimédienne, tout élément non-nul de k_v s'appelle une *unité* de k_v. Dans les deux cas, l'ensemble des unités se note U_v. (Donc si v est non-archimédienne et P-adique on a $U_v = U_P$, et si v est archimédienne on a $U_v = k_v^\times$. Il est clair que U_v forme un groupe multiplicatif.) Ce qu'on appelle maintenant *idèle* de k est un élément $(\cdots \alpha_v \cdots)$ du produit direct $\prod_v k_v^\times$ où v parcourt toutes les places de k, dont les composants α_v sont les unités de k_v sauf pour un nombre fini de v. (On dit aussi: *presque tous* les composants sont les unités.) L'ensemble de tous les idèles de k se notera J_k. Pour deux idèles $\alpha = (\cdots \alpha_v \cdots), \beta = (\cdots \beta_v \cdots)$ on définit le produit $\alpha\beta = (\cdots \alpha_v\beta_v \cdots)$. Il est clair que J_k forme un groupe multiplicatif. L'ensemble des idèles dont tous les composants $\alpha_v \in U_v$ pour toutes les places v, forme évidemment un sousgroupe de J_k qui sera noté U. Un élément de U s'appellera *unité* de J_k.

Si $a \in k^\times$, on a $a \in U_v$ pour toutes les places archimédiennes v et $e_P(a) \neq 0$ n'a lieu que pour un nombre fini d'idéaux premiers de k qui paraissent comme diviseurs premiers de (a). On peut donc concevoir un élément α de J_k, dont tous les composants α_v sont égal à a. On l'identifiera avec a. Ainsi $k^\times$ est plongé dans J_k comme un sousgroupe. Les idèles dont tous les composants soit égaux à un élément de $k^\times$ s'appellent les *idèles principaux*. Le sousgroupe de J_k formé par ceux-ci sera nommé le *sousgroupe principal* et désigné par P_k. On a évidemment $P_k \cong k^\times$.

Soit F le groupe des idéaux fractionnaires de k. A tout idèle $\alpha \in J_k$, on peut faire correspondre un élément de F comme suit. Soient $v_1, \ldots, v_\lambda$ toutes les places pour lesquelles $\alpha_{v_i} \notin U_{v_i}$. Toutes ces v_i sont non-archimédiennes. Soient $P_1, \ldots, P_\lambda$ les idéaux premiers correspondant à ces places. Posons $e_{P_i}(\alpha) = e_i, i = 1, \ldots, \lambda$ et $A = P_1^{e_1} \cdots P_\lambda^{e_\lambda}$. Il est évident que cette application $j : \alpha \to A$ de J_k à F est un homomorphisme, avec le noyau U: $J_k/U \cong F$. Nous appellerons j l'*application canonique* de J_k à F.

Enfin, v étant une place de k, un idèle $\alpha \in J_k$ avec $\alpha_{v'} = 1$ pour tout $v' \neq v$ s'appellera *primaire pour* v. Un tel idèle peut s'identifier avec $\alpha_v \in k_v^\times$. Ainsi $k_v^\times$ se trouve plongé dans J_k.

Soit maintenant K une extension finie de k. Chaque place v de k se prolonge à une place $\bar{v}$ de K et inversement chaque place de K est un prolongement d'une place de k. Le corps local $K_{\bar{v}}$ est une extension finie de k_v, et ainsi le groupe d'idèle J_k est plongé dans J_K.

Si σ est un isomorphisme de k à son conjugué k^σ, il est clair qu'à toute place v de k correspond une place v^σ de k^σ, et à tout corps local k_v correspond un corps local k_{v^σ}, et donc enfin à J_k le groupe d'idèles J_{k^σ} de k^σ.

Pour une extension finie K de k, soit $\tilde{K}$ une extension galoisienne de k contenant K avec le groupe de Galois $G(\tilde{K}/k) = \{\sigma_1, \ldots, \sigma_m\}$. K a alors les conjugués K^{σ_i}, $i = 1, \ldots, m$ contenus dans $\tilde{K}$, et le groupe d'idèles J_K a ses conjugués $J_{K^{\sigma_i}}$, contenus dans $J_{\tilde{K}}$. On peut multiplier un idèle $\bar{\alpha} \in J_K$ avec ses conjugués $\bar{\alpha}^{\sigma_i}$ dans $J_{\tilde{K}}$. Le produit $\prod_{i=1}^m \bar{\alpha}^{\sigma_i}$ est un idèle de $J_{\tilde{K}}$ invariant par

$\sigma_i, i = 1, \ldots, m$, qui s'identifie, comme il est facile à voir, avec un idèle α de J_k. On appelle cet idèle α la *norme* (relative) de $\bar{\alpha} \in J_K$ à J_k et écrit $\alpha = N_{K/k}(\bar{\alpha})$. Il est clair que l'application $N_{K/k}$ ainsi définie donne un homomorphisme de J_K à J_k.

Si, de plus, $\bar{\alpha} \in P_K$, on voit immédiatement $N_{K/k}\bar{\alpha} \in P_k$, de sorte que $N_{K/k}$ applique J_K/P_K homomorphiquement dans J_k/P_k. On appelle les élément de J_k/P_k les *classes d'idèles*, et le groupe quotient J_k/P_k le groupe des classes d'idèles de k. On le désigne par C_k. Il est clair que C_K est appliqué homomorphiquement dans C_k par $N_{K/k}$.

Le "théorème réciproque" de la théorie du corps de classes (*cf.* supra p.38) s'énonce alors comme suit:

Si K/k est une extension abélienne, on a

$$J_k/P_kN_{K/k}(J_K) = C_k/N_{K/k}(C_K) \cong \mathrm{Gal}(K/k)$$

et une place v de k ne se ramifie pas dans K si et seulement si $U_v \subseteq P_kN_{K/k}(J_K)$.

Ainsi on peut éviter la difficile terminologie des groupes d'idéaux avec les modules de définition dans cette élégante formulation idélique.

*

Pour formuler le "théorème d'existence" il faut tenir compte de la topologie de J_K. Les corps locaux k_v sont des espaces métrisés par la distance $d(a,b) = \varphi(a-b)$, donc topologique, Hausdorff et localement compacts, comme il est facile à constater. Le groupe abélien d'idèle J_k forme un sousespace de $\prod_v k_v$ muni de la toplogie de l'espace produit et on voit sans difficulté que J_k est un groupe abélien, localement compact sur lequel la théorie de dualité d'après Pontrjagin est valable (*cf.* Pontrjagin [1]). On voit que P_k est un sousgroupe fermé de J_k et donc $C_k = J_k/P_k$ est aussi un groupe abélien localement comapct.

Soit maintenant K/k une extension abélienne de degré fini n. On voit alors que $P_kN_{K/k}(J_K)$ et $N_{K/k}(C_K)$ sont les sousgroupes fermés de J_k et de C_k d'un indice fini n, respectivement. Le "théorème d'existence" dit que "la réciproque est vraie " dans le sens suivant:

Soit H un sousgroupe fermé d'indice fini n de J_k, ou bien un sousgroupe fermé d'indice fini n de C_k. Alors il y a une extension abélienne K/k de degré fini n telle qu'on ait

$$H = P_kN_{K/k}(J_K)$$

ou

$$H = N_{K/k}(C_K),$$

respectivement.

On a vu que la loi générale de réciprocité d'Artin dans la formulation classique explicite l'isomorphie entre $G(K/k)$ et $F/H : C$ étant le conducteur de K/k, H contient le rayon R_C modulo C, et à tout idéal A relativement premier

à C, correspond le symbole d'Artin $\left(\frac{K/k}{A}\right)$ dont la valeur dans $G(K/k)$ ne dépend que de la classe de $A \bmod H$, et la correspondance (classe de $A \bmod H$) $\leftrightarrow \left(\frac{K/k}{A}\right)$ explicite cet isomorphisme.

Pour la formulation idélique de cette loi, Chevalley considère encore les congruences entre les idèles modulo les diviseurs $M = P_1^{e_1} \cdots P_g^{e_g}$ dans son mémoire [5] de 1936: on a $\alpha \equiv \beta \,(\bmod M)$ pour deux idèles $\alpha, \beta \in J_k$ si et seulement si $e_{P_i}(\alpha\beta^{-1} - 1) \geq e_i$ si P_i est non-archimédienne et $\alpha\beta^{-1}$ est positif dans k_v si P_i est archimédienne correspondant à k_v réel (et $e_i = 1$). Soit C le conducteur de K/k. On voit alors facilement que tout idèle $\alpha \in J_k$ se met sous la forme $\alpha = a\alpha_1, a \in P_k, \alpha_1 \equiv 1 \,(\bmod C)$ et la valeur de $\left(\frac{K/k}{j(\alpha_1)}\right)$ ne dépend pas de la décomposition de α en $a\alpha_1$ (où j désigne l'application canonique de J_k à F). On pose alors $\left(\frac{K/k}{\alpha}\right) = \left(\frac{K/k}{j(\alpha_1)}\right)$ et constate que ce symbole explicite l'isomorphisme de $J_k/P_k N_{K/k}(J_K)$ avec $G(K/k)$ et que le diagramme suivant est commutatif, si K' est un corps intermédiaire de K/k:

$$(*) \qquad \begin{array}{ccc} J_k/P_k N_{K/k}(J_K) & \xrightarrow{\left(\frac{K/k}{\alpha}\right)} & G(K/k) \\ \downarrow{\scriptstyle \theta'} & & \downarrow{\scriptstyle \theta} \\ J_k/P_k N_{K'/k}(J_{K'}) & \xrightarrow[\left(\frac{K'/k}{\alpha'}\right)]{} & G(K'/k) \end{array}$$

où $\theta' : J_K \longrightarrow J_{K'}$ est l'application naturelle, $\theta : G(K/k) \longrightarrow G(K'/k)$ l'application usuelle et $\alpha' = \theta'(\alpha)$.

*

Dans ce mémoire [5], Chevalley avait pour but de généraliser la théorie du corps de classes pour les extensions infinies, comme le titre indique. Pour cela, il faut utiliser la théorie de Galois pour les extensions infinies, établie par Krull [1] vers la fin des 1920 moyennant l'idée des groupes topologiques, comme on l'expliquera ci-dessous par la notion de la limite projective (ou inverse). (*cf.* Eilenberg–Steenrod [1] Chap.XIII)

Soit k une clôture algébrique de k et $\bar{k}^a$ la réunion de toutes les extensions abéliennes de k contenues dans $\bar{k}$. On appellera $\bar{k}^a$ une *clôture abélienne* de k. Toute extension abélienne finie K de k, jusqu'ici considérée, s'identifie avec une extension intermédiaire entre $\bar{k}^a$ et k. La théorie du corps de classes, la loi générale de réciprocité en particulier, donne une isomorphie explicite entre $G(K/k)$ et $J_k/P_k N_{K/k}(J_K)$ ou $C_k/N_{K/k}(C_K)$, ces derniers construits à l'intérieur du corps de base k. k^a étant évidemment une extension galoisienne de k, une

explicitation de l'isomorphie de $G(\bar{k}^a/k)$ avec une structure intérieure convenablement définie dans k établierait d'un seul coup la théorie entière du corps de classes sur k.

Pour expliquer comment Chevalley l'a montré, récapitulons d'abord la théorie des systèmes inductifs ou projectifs et des limites inductives ou projectives.

*

Soit I un ensemble dirigé, c'est-à-dire un ensemble partiellement ordonné par $\leq$ de sorte que pour tout couple $i, j \in I$, il y ait un $\ell \in I$ tel que $i \leq \ell, j \leq \ell$. Supposons qu'il y ait un ensemble de structures du même type (par exemple: groupes, corps, espaces topologiques, etc.) indexées par I de telle sorte qu'il y ait un morphisme $\varphi_{ij} : A_i \to A_j$ (ou $\varphi_{ij} : A_j \to A_i$) tel que $\varphi_{ii} = \mathrm{id}_{A_i}$ et $\varphi_{jl}\varphi_{ij} = \varphi_{il}$ (ou $\varphi_{ij}\varphi_{jl} = \varphi_{il}$) si $i \leq j \leq l$. On dit alors que (I, A_i, φ_{ij}) constitue un *système inductif* (ou *système projectif*), et on définit la limite inductive $\varinjlim A_i$ (ou la limite projective $\varprojlim A_i$) comme suit:

Soit A la somme directe $\coprod_i A_i$ (ou le produit direct $\prod_i A_i$). La *limite inductive* $\varinjlim A_i$ (ou la *limite projective* $\varprojlim A_i$) est le quotient de A par rapport à l'équivalence $a_i \sim a_j$ où $a_i \in A_i, a_j \in A_j$ et $\varphi_{i\ell}(a_i) = \varphi_{j\ell}(a_j)$ pour un $\ell \in I$ tel que $i \leq \ell, j \leq \ell$ (ou le sous-ensemble $\{(\ldots, a_j, \ldots) \in A; \varphi_{j\ell}(a_\ell) = a_j \text{ si } j \leq \ell\}$ de A). Pour chaque $j \in I$, il y a alors une application $\varphi_j : A_j \to \varinjlim A_i$ (ou $\varphi_j : \varprojlim A_i \to A_j$) définie par l'injection $A_j \to A$ (ou la projection $A \to A_j$). On a alors évidemment $\varphi_j \varphi_{ij} = \varphi_i$ (ou $\varphi_{ij}\varphi_j = \varphi_i$).

Supposons que A_i soient espaces topologiques de Hausdorff. A est alors muni de la topologie du produit direct qui induit une topologie à son sous-espace $\varinjlim A_i$ (ou $\varprojlim A_i$). On voit que $\varinjlim A_i$ (ou $\varprojlim A_i$) est fermé dans A, en supposant bien entendu que φ_{ij} (où φ_{ji}) soient continues.

Supposons maintenant que A_i soient finis avec topologie discrète. A est alors discret (ou compact), donc $\varinjlim A_i$ (ou $\varprojlim A_i$) l'est aussi. Il est facile à voir que $\varprojlim A_i$ n'est pas vide et qu'il est totalement discontinu. La limite projective des structures finies s'appelle *profinie*; en particulier, la limite projective des groupes finis s'appelle le *groupe profini*. Celui-ci est compact et totalement discontinu comme on l'a vu, et on montre réciproquement que tout groupe compact et totalement discontinu est un groupe profini.

Retournons maintenant à nos extensions galoisiennes infinies $\bar{k}$ et $\bar{k}^a$ d'un corps de nombres algébriques k. Ces extensions peuvent être évidemment considérées comme les limites inductives des extensions algébriques ou abéliennes finies k_i de k contenues dans $\bar{k}$ ou $\bar{k}^a$. Comme le système indexant, on peut choisir $\{k_i\}$ et comme $\varphi_{ij} : k_i \to k_j$ les injections canoniques de k_i dans $k_j \supset k_i$. Les groupes de Galois $G(\bar{k}/k)$ et $G(\bar{k}^a/k)$ se définissent alors comme les limites projectives $\varprojlim G(k_i/k)$ des systèmes projectifs $G(k_i/k)$ avec les systèmes

indexants $\{k_i\}$ comme auparavant avec $k_i \subset \bar{k}$, k_i/k galoisienne, ou $\subset \bar{k}^a$, et $\varphi_{ij} : G(k_j/k) \to G(k_i/k)$ pour $k_i \subset k_j$, projections canoniques des groupes de Galois. $G(\bar{k}/k)$ et $G(\bar{k}^a/k)$ sont donc les groupes profinis dont chaque sous-groupe fermé stabilise un corps intermédiaire k_i de k/k ou de $\bar{k}^a/k$, de degré fini sur k, respectivement.

Soit α un élément de J_k. Il y a alors un élément σ de $G(\bar{k}^a/k)$ tel qu'on ait $\left(\frac{k_i/k}{\alpha}\right) = \sigma$ pour tous les k_i avec $\varinjlim k_i = \bar{k}^a$. En effet, si l'on pose $\sigma_i = \left(\frac{k_i/k}{\alpha}\right) \in G(k_i/k), \sigma_j\sigma_i^{-1}$ pour $j > i$ laisse invariant en vertu de la commutativité du diagramme $(*)$, tout élément le k_i, et donc σ_i, converge à un élément σ de $G(\bar{k}^a/k)$. On n'a qu'à poser $\left(\frac{\bar{k}^a/k}{\alpha}\right) = \sigma$. On montre que l'application $\psi : J_k \to G(\bar{k}^a/k)$ définie par $\psi(\alpha) = \left(\frac{\bar{k}^a/k}{\alpha}\right)$ est surjective et applique J_k/D_k à $G(\bar{k}^a/k)$ où $D_k = \operatorname{Ker}\psi$. Il se révèle que D_k coïncide avec la composante connexe de J_k autour de 1, de sorte que le résultat essentiel de la théorie du corps de classes se résume en termes suivants:

Le symbole $\left(\frac{\bar{k}^a/k}{\alpha}\right) = \sigma$ *établit une isomorphie topologique entre* J_k/D_k *et le groupe de Galois* $G(\bar{k}^a/k)$. *Si* K *est une extension abélienne de* k *de degré fini, il s'identifie avec un corps intermédiaire de* $\bar{k}^a/k$ *et le groupe* $H_{K/k} = P_k N_{K/k}(J_K)$ *se compose des* $\alpha \in J_k$ *tel que* $\left(\frac{\bar{k}^a/k}{\alpha}\right) \in G(\bar{k}^a/K)$ *et inversement le groupe de Galois* $G(\bar{k}^a/K)$ *coïncide avec l'ensemble de* $\left(\frac{\bar{k}^a/k}{\alpha}\right)$ *avec* $\alpha \in H_{K/k}$.

L'extension abélienne K de k et le sousgroupe fermé $H_{K/k}$ intermédiaire de J_k/D_k se définissent ainsi mutuellement. On a de plus un théorème d'existence:

Le famille des groupes $H_{K/k}$ *pour les diverses extensions abéliennes* K *de* k *coïncide avec la famille des sousgroupes fermés de* J_k *contenant* D_k.

C'est avec ces théorèmes que Chevalley conclut son mémoire [5] de 1936.

*

Chevalley donne une démonstration arithmétique de ces résultats dans son mémoire [6] de 1940. Il le fait en utilisant la théorie de la dualité des groupes abéliens localement compacts, c'est-à-dire celle des caractères de ces groupes selon Pontrjagin (*cf.* Pontrjagin [1]). Rappelons en d'abord quelques faits fondamentaux.

Le caractère χ d'un groupe abélien G est une application homomorphe de G dans le groupe multiplicatif Γ des nombres complexes de valeur absolue 1;

$\chi : G \to \Gamma$. L'ensemble de ces caractères forme un groupe abélien $\widehat{G}$, dit *groupe dual* de G. Quand G est un groupe topologique, on suppose χ continus et que $\widehat{G}$ est muni de la topologie de la convergence compacte. Si G est un groupe (abélien) localement compact, le groupe dual $\widehat{G}$ l'est aussi, et on montre que G est $\widehat{\widehat{G}}$ sont canoniquement isomorphes comme groupes topologiques.

Soit k un corps de nombres algébriques et $\overline{k}^a$ une clôture abélienne de k comme auparavant et $G = G(\overline{k}^a/k)$. G est alors un groupe abélien profini, donc compact et totalement discontinu, auquel s'applique la théorie de Pontrjagin, et on voit de plus que tout caractère $\chi \in \widehat{G}$ est d'ordre fini.

Soit $\chi \in \widehat{G}$. Le sousgroupe G_χ de G défini par $G_\chi = \{\sigma \in G; \chi(\sigma) = 1\}$ est un sousgroupe fermé d'indice fini de G auquel correspond un corps intermédiaire k_χ de $\overline{k}^a/k$. Le groupe de Galois $G(k_\chi/k)$ est alors isomorphe au G/G_χ qui s'applique isomorphiquement par χ sur un sousgroupe fini, donc cyclique de Γ. Ainsi k_χ/k est une extension finie cyclique. Inversement, toute extension finie cyclique de k s'exprime évidemment comme k_χ avec $\chi \in \widehat{G}$.

Considérons maintenant une extension finie K/k. Une clôture abélienne $\overline{K}^a$ de K contient alors $\overline{k}^a$ et K, et tout élément $\overline{\sigma}$ de $G(\overline{K}^a/K)$ appliqué sur les éléments de $\overline{k}^a$ donne un élément σ de $G(\overline{k}^a/k)$. Cette application $\overline{\sigma} \to \sigma$ de $G(\overline{K}^a/K)$ à $G(\overline{k}^a/k)$ qui est évidemment un homomorphisme continu, sera notée $\Psi_{K/k} : G(\overline{K}^a/K) \to G(\overline{k}^a/k)$. Soit χ un caractère de $G(\overline{k}^a/k)$, c'est-à-dire un élément de $\widehat{G}(\overline{k}^a/k)$. χ induit alors un caractère $\overline{\chi}$ de $G(\overline{K}^a/K)$, qui fait correspondre à $\overline{\sigma} \in G(\overline{K}^a/K)$, $\overline{\chi}(\overline{\sigma}) = \chi(\sigma)$ où $\sigma = \Psi_{K/k}(\overline{\sigma})$. L'application $\chi \to \overline{\chi}$ de $\widehat{G}(\overline{k}^a/k)$ à $\widehat{G}(\overline{K}^a/K)$ est évidemment aussi un homomorphisme continu qu'on notera $\Phi_{k/K}$. Si on a $k \subset K_1 \subset K$, il est clair qu'on a $\Phi_{k/K} = \Phi_{K_1/K}(\Phi_{k/K_1})$. (Chevalley [6] note $N_{k/K}$ au lieu de $\Phi_{k/K}$.)

Dans le §3 du mémoire [6], Chevalley définit comme suit une "topologie multiplicative" pour le groupe J_k des idèles de k.

Soient E un ensemble fini des places de k archimédiennes ou non-archimédiennes, et n un entier positif. On notera $J_k^{E,n}$ le sous-ensemble de J_k qui se compose des idèles α satisfaisant aux conditions suivantes: 1) si $v \notin E$, α_v est une unité de k_v, 2) si $v \in E$, on distingue trois cas: 2.1) si v est archimédienne et réelle, $\alpha_v > 0$; 2.2) si v est archimédienne et complexe, on n'impose aucune condition à α_v; 2.3) si v est non-archimédienne, il faut qu'on ait $\alpha_v \in (k_v^\times)^n$. On voit que les sous-ensembles $G_k^{E,n} = J_k^n J_k^{E,n}$ où $J_k^n = \{\alpha^n; \alpha \in J_k\}$ et où E, n parcourent tous les ensembles finis des places de k et tous les entiers positifs, respectivement, constituent une famille fondamentale des voisinages d'une topologie (d'ailleurs non séparée) de J_k, pour laquelle l'application $(\alpha, \beta) \to \alpha\beta^{-1}$ de $J_k \times J_k$ à J_k est continue. Dans le mémoire, Chevalley a considéré J_k comme un groupe topologique munie de cette topologie [6]. Alors tout marche bien comme indiqué dans ce mémoire, mais on s'est aperçu plus tard qu'il vaut mieux

remplacer cette topologie par celle qui est définie en p.62. Nous regarderons dorénavant J_k muni de cette dernière topologie.

Si en particulier, K/k est une extension finie, l'application $N_{K/k}$ de J_K à J_k dont on a parlé plus haut, sera alors une application continue.

Soit maintenant $a \in k^\times$. Pour chaque place v de k, on définit $w_v(a)$ comme suit: si v est archimédienne et réelle, on pose $w_v(a) = |I_v(a)|$ où I_v est l'isomorphisme de k au corps conjugué réel de k correspondant à v; si v est archimédienne et complexe, il y a deux corps conjugués complexes de k qui lui correspondent, donc deux isomorphismes I_v, I'_v de k à ces corps; on pose alors $w_v(a) = |I_v(a) \cdot I'_v(a)| = |I_v(a)|^2$; si v est non-archimédienne et correspond à P, on posera $w_v(a) = |NP|^{-n}$, où $n = e_P(a)$. On aura alors

$$|Na| = \prod_{v\text{: arch.}} w_v(a) = \prod_{v\text{: non-arch.}} w_v(a)^{-1},$$

de sorte qu'on ait

$$\prod_v w_v(a) = 1$$

où v parcourt toutes les places de k.

Moyennant ces valeurs de $w_v(a)$, on peut démontrer le résultat suivant:

Etant donnés un $a \in k^\times$ et les nombres positifs $c_v > 0$ pour chaque place v de k tels que 1) $c_v = 1$ pour presque tous les v, 2) $c_v = w_v(a)$ pour toutes les v non-archimédiennes et 3) $\prod_v c_v \geq |D_k|^{1/2}$ où D_k est le discriminant de k, il existe un $a' \in k^\times$ satisfaisant à toutes les inégalités $w_v(a') \leq c_v$.

Il est facile de voir qu'il n'existe qu'un nombre fini de $a' \in k^\times$ satisfaisant à ces inégalités, et ce résultat entraîne les corollaires: (1) *Si E est un ensemble fini de places contenant toutes les places archimédiennes, $P_k J_k^{E,1}$ est d'indice fini dans J_k*, et (2) *Il existe un ensemble fini F de places de k tel que $P_k J_k^{F,1} = J_k$.*

Ecrivons $P_k^E = P_k \cap J_k^{E,1}$ et supposons que E consiste de $h+1$ places et contient toutes les places archimédiennes de k. En utilisant les mêmes arguments que pour démontrer le théorème de Dirichlet sur la structure du groupe des unités de corps de nombres algébriques, on montre qu'on peut faire correspondre un nombre $\varepsilon_v \in P_k^E$ à chaque place $v \in E$ de sorte qu'on ait $w_{v'}(\varepsilon_v) < 1$ pour tout $v' \neq v$ et qu'ils engendrent un sousgroupe d'indice fini de P_k^E, et tels qu'aucun sous-ensemble de h de ces nombres ne soit lié par une relation multiplicative, c'est-à-dire que si $v_i, i = 1, 2, \ldots, h$ sont h places quelconques de E, une relation de la forme $\varepsilon_{v_1}^{\nu_1} \cdots \varepsilon_{v_h}^{\nu_h} = 1$, $\nu_1, \ldots, \nu_h \in \boldsymbol{Z}$ entraîne nécessairement $\nu_1 = \cdots = \nu_h = 0$. Il s'ensuit de là que P_k^E est un produit direct d'un groupe abélien fini et d'un groupe abélien libre à $h+1$ générateurs. Comme on sait que les éléments d'ordres finis de P_k^E sont les racines de l'unité de k, on voit que l'indice de $(P_k^E)^n$ dans P_k^E est n^{h+1}, si k contient une racine primitive n-ième de l'unité.

Chevalley appelle une *différentielle* de k un élément de $\widehat{J}_k$, groupe dual de J_k, qui est identiquement égal à 1 sur P_k et d'ordre fini. Elles forment évidemment un groupe multiplicatif qu'on notera $\mathscr{D}_k$.

Un élément ψ de $\widehat{J}_k$ qui n'est pas identiquement égal à 1 sur le groupe U_v des unités de k_v^* est dit *ramifié* à v. Pour un $\psi \in \widehat{J}_k$ donné, on notera ψ_v l'élément de $\widehat{J}_k$ qui s'identifie avec ψ sur k_v^* et est égal à 1 sur tous les $k_{v'}^*$, pour $v' \neq v$, et l'appellera la *v-coordonnée* de ψ. Comme il n'y a qu'un nombre fini de places où ψ est ramifié, on peut démontrer qu'une différentielle est entièrement déterminée par la donnée de presque toutes ses coordonnées.

Considérons maintenant une extension finie K/k. Soient φ une différentielle de k, et $\bar{\alpha} \in \widehat{J}_K$. Alors $\bar{\varphi}(\bar{\alpha})$ défini par $\varphi(N_{K/k}(\bar{\alpha}))$ est évidemment une différentielle de K qu'on notera $\Phi_{k/K}(\varphi)$. Si on a $k \subset K_1 \subset K$, il est clair qu'on a $\Phi_{k/K} = \Phi_{k_1/K}(\Phi_{k/K_1})$. Et si τ est un isomorphisme de K à l'un de ses conjugués K^τ, il est clair aussi que l'application $\bar{\varphi}^\tau : J_{\bar{K}^\tau} \to \Gamma$ définie par $\bar{\varphi}^\tau(\bar{\alpha}^\tau) = \bar{\varphi}(\bar{\alpha})$ est une différentielle de K^τ, et l'application $\bar{\varphi} \to \bar{\varphi}^\tau$ établit un isomorphisme de $\mathscr{D}_K$ à $\mathscr{D}_{K^\tau}$.

Moyennant ces définitions et ces notations, les théorèmes centraux de la théorie du corps de classes s'énoncent ainsi:

k étant un corps de nombres algébriques de degré fini, il existe un isomorphisme Φ_k du groupe de caractères $\widehat{G}$ du groupe de Galois $G = G(\bar{k}^a/k)$ de la clôture abélienne k^a sur k au groupe $\mathscr{D}_k$ des différentielles de k, jouissant des propriétés suivantes:

I. *Si K/k est une extension finie, on a*

$$\Phi_K(\Phi_{k/K}(\chi)) = \Phi_{k/K}(\Phi_k(\chi)).$$

II. *Si τ est un isomorphisme de K à l'un de ses conjugués K^τ sur k, on a*

$$\Phi_{K^\tau}(\chi^\tau) = (\Phi_K(\chi))^\tau.$$

III. *Les places de ramification de $\chi \in \widehat{G}$ et de $\Phi_k(\chi)$ sont les mêmes. (On dit qu'un élément de $\widehat{G}$ est ramifié à la place v de k si v est ramifié dans Z_χ.)*

La propriété I montre qu'on a $\varphi(N_{Z_\chi/k}(\bar{\alpha})) = 1$ pour tout idèle $\bar{\alpha}$ de Z_χ si $\varphi = \Phi_k(\chi)$. Si Z/k est une extension abélienne, on dira donc qu'une différentielle $\varphi \in \mathscr{D}_k$ est *associée* à l'extension abélienne Z de k si $\varphi(N_{Z/k}(\bar{\alpha})) = 1$ pour tout idèle $\bar{\alpha}$ de Z. Une telle extension Z étant donnée, les différentielles qui y sont associées forment un groupe. Si Z/k est cycliques, on montre que les ordres des groupes des différentielles qui y sont associées sont multiples de $(Z : k)$. Ceci correspond à ce qu'on a appelé plus haut la première inégalité de notre théorie. On montre aussi que l'ordre du groupe des différentielles associées à une extension abélienne finie quelconque Z/k est au plus égal à $(Z : k)$, ce qui correspond à la deuxième inégalité. Dans la théorie classique, on a démontré la première inégalité par une méthode analytique, puis la deuxième inégalité

par une méthode arithmétique dont l'origine remonte à Gauss. Dans la nouvelle démonstration dans ce mémoire, on démontre d'abord la "deuxième inégalité" par une méthode qui est essentiellement la même qu'auparavant et ensuite la "première inégalité" en employant le résultat de la "deuxième inégalité". Tout se fait ici arithmétiquement.

Dans la démonstration des théorèmes centraux, on utilise les *caractères locaux non ramifiés* $(*,\chi)_v$ définis comme suit: On se donne un corps de nombres algébriques de degré fini k une fois pour toutes et ne l'explicitera plus chaque fois. Soit v une place non-archimédienne et $\chi \in \widehat{G}$ où $G = G(\bar{k}^a/k)$. On suppose que χ est non ramifié à v. Z_χ est alors une extension cyclique de k et $G(Z_\chi/k)$ contient un élément, dit *substitution de Frobenius* $(Z_\chi/k)_v$ attachée à v, satisfaisant à

$$(Z_\chi/k)_v\theta \equiv \theta^{n_v} \pmod{v}$$

où n_v est la norme absolue de v et θ est un entier quelconque de Z_χ. On posera

$$(\alpha,\chi)_v = \chi(Z_\chi/k)_v^\nu$$

pour $\alpha \in J_k$, où ν est l'ordre de α pour v. On écrira $(*,\chi)_v$ avec le signe $*$ pour indiquer la position de la variable $\alpha \in J_k$. Ceci est évidemment un caractère local non ramifié de J_k, qui engendre le groupe de décomposition de v pour Z_χ/k, dont l'ordre est donc égal à l'ordre de ce groupe. On constate de plus les formules:

$$(\alpha,\chi\chi')_v = (\alpha,\chi)_v(\alpha,\chi')_v,$$

$$(\alpha,\chi^\tau)_{v^\tau} = (\alpha,\chi)_v,$$

où τ est un isomorphisme de k avec l'un de ses conjugués. Et si K/k est une extension finie, et $\bar{\alpha} \in J_K$, on a

$$(N_{K/k}\bar{\alpha},\chi)_v = \prod_{\bar{v}}(\bar{\alpha},\Phi_{k/K}\chi)_{\bar{v}}$$

où $\bar{v}$ parcourt les places de K sur v.

Dans la dernière étape de démonstration, on emploie comme dans les démonstrations antérieures la "méthode de croisement" avec les corps circulaires.

On dit qu'un caractère χ est *circulaire*, si l'extension Z_χ/k est contenue dans $k(\zeta)/k$ où ζ est une racine de l'unité dont l'ordre sera noté m. Soit E l'ensemble de toutes les places archimédiennes et des places où m est ramifié. Si n est l'ordre de χ et a $(\in K)$ appartient à tous les $(k_v)^n$ où $v \in E$, on démontre qu'on a la "formule de produit"

$$\prod_{v\in E}(a,\chi)_v = 1.$$

En vertu de cette belle formule, on peut construire une différentielle φ_χ de k pour un χ circulaire: Pour $\alpha \in J_k$, on peut trouver un "nombre auxiliaire" $b \in k^*$ tel que $(\alpha b^{-1})_v \in (k_v)^n$ pour tous les $v \in E$. Il suffit de poser

$$\varphi_\chi(\alpha) = \prod_{v \in E} (\alpha b^{-1}, \chi)_v.$$

La formule de produit assure que le second membre ne dépend pas du choix de b, et la fonction $\varphi_\chi(\alpha)$ ainsi définie est effectivement une différentielle associée à Z_χ/k. Elle est caractérisée par les propriétés suivantes:

I. *L'application $\chi \to \varphi_\chi$ est un homomorphisme (injectif) du groupe des caractères circulaires dans $\mathscr{D}_k$.*

II. *K/k étant une extension finie, χ un caractère circulaire de $G(\bar{k}^a/k)$, on a*

$$\varphi_{\Phi_{k/K}(\chi)} = \Phi_{k/K}(\varphi_\chi).$$

($\Phi_{k/K}(\chi)$ est un caractère circulaire de $G(\bar{K}^a/K)$.)

Pour assurer la possibilité de "croisement" on a encore besoin du lemme suivant (qui équivaut au "théorème d'existence" dans le Chap.VII de la Thèse [2] de Chevalley. Cf. supra p.58):

Soient v une place non archimédienne de k, n un entier positif, K/k une extension finie. Il existe alors un caractère circulaire χ de $G(k^a/k)$ non ramifié en v tel que $(*, \chi)_v$ soit d'ordre n et $Z_\chi \cap K = k$.

Après ces préparatifs, on construit comme suit l'isomorphisme cherché Φ_k : $\widehat{G} \to \mathscr{D}_k$, où $G = G(\bar{k}^a/k)$ et $\mathscr{D}_k$ est le groupe des différentielles de k.

On utilisera la locution suivante: Les éléments $\chi, \chi', \ldots$ de $\widehat{G}$ seront dits *indépen-dants* si $\chi^\nu \chi'^{\nu'} \cdots = 1$, $\nu, \nu', \ldots \in \boldsymbol{Z}$ entraîne $\nu = \nu' = \cdots = 0$. Si $Z_\chi/k, Z_{\chi'}/k, \ldots$ sont les extensions associées correspondantes, l'indépendance de $\chi, \chi', \ldots$ signifie que l'intersection de chacun des corps $Z_\chi, Z_{\chi'} \ldots$ avec le corps composé de tous les autres corps se réduit à k.

Soit $\chi \in \widehat{G}$ d'ordre n, et $\varphi \in D_k$ associé à Z_χ/k. Soit χ' un caractère circulaire de G, indépendant de χ, dont l'ordre est un multiple de n, et $\varphi' \in D_k$ associé à χ', et posons $K' = Z_{\chi\chi'^a}$ où a est un entier. L'extension $K'Z_\chi/K'$ est alors cyclique et circulaire. La différentielle associée à $\Phi_{k/K'}(\chi'^{-a})$ est alors $\Phi_{k/K'}(\varphi'^{-a})$ et comme $\Phi_{k/K'}(\varphi)$ est une différentielle associée à $Z_\chi K'/K'$, il existe un entier b tel que $\Phi_{k/K'}(\varphi) = \Phi_{k/K'}(\varphi'^b)$. On va montrer qu'il existe un entier c tel que $b \equiv ac \pmod{n}$.

On introduit pour cela un élément χ'' de $\widehat{G}$, dont l'ordre est un multiple de n tel que χ, χ', χ'' soient indépendants. Posons $K'' = Z_{\chi\chi''}$ et soit φ'' la différentielle associée à χ''. On voit comme tout à l'heure qu'il y a un entier c tel qu'on ait $\Phi_{k/K''}(\varphi) = \Phi_{k/K''}(\varphi''^c)$.

On considère l'extension $K'K''/K''$ à laquelle $\Phi_{k/K''}(\varphi\varphi'^{-a}) = \Phi_{k/K''}(\varphi''^c \varphi'^{-a})$ est associée, comme la différentielle $\varphi\varphi'^{-a}$ est associée à K''/k. Mais

$\Phi_{k/K''}(\varphi''^c\varphi'^{-a})$ est la différentielle associée au caractère circulaire $\Phi_{k/K''}(\chi''^c\chi'^{-a})$. D'autre part, le caractère circulaire $\Phi_{k/K''}(\chi\chi'^a) = \Phi_{k/K''}(\chi''^{-1}\chi'^{-a})$ est un caractère primitif du groupe de Galois $G(K'K''/K'')$, donc $\Phi_{k/K''}(\chi''^c\chi'^{-a})$ se met sous la forme $\Phi_{k/K''}(\chi''^{-1}\chi'^{-a})^x$ de sorte que

$$\chi''^c\chi'^{-a} = (\chi''^{-1}\chi'^{-a})^x(\chi\chi'')^y$$

d'où l'on tire $b \equiv ac \pmod n$.

Soit maintenant v une place non-archimédienne non ramifiée dans Z. D'après ce qu'on a vu, il y a un caractère circulaire χ de G tel que φ'_v soit un caractère non-ramifié d'ordre n, de sorte que $(*,\chi)_v$ est aussi un caractère non-ramifié de k_v^* dont l'ordre est un multiple de n. $(*,\chi)_v$ pourra donc se mettre sous la forme $(\varphi'_v)^c$, $c \in \boldsymbol{Z}$. On aura donc $(*,\chi\chi'^c)_v = 1$ et par suite $K'k_v = k_v$, $\varphi_v = \varphi'^a_v$. Comme on a d'autre part $a \equiv bc \pmod n$ on obtient $\varphi_v = (*,\chi')_v^{-a} = (*,\chi')_v^{bc} = (*,\chi')^b$.

Si l'on convient de dire que b est un *entier coordonné* à la différentielle φ associée à Z_χ/k, lorsque pour presque toutes les places non-archimédiennes non-ramifiées dans Z_χ on a $\varphi_v = (*,\chi)^b$, on voit que les deux différentielles φ, φ_1 associées à Z_χ coïncident dès que leurs coordonnés coïncident mod n. Comme il y a n différentielles distinctes associées à Z_χ, il y en a une et une seule à laquelle $1 \bmod n$ soit coordonné. C'est celle-ci qu'on appellera *la différentielle associée à* χ et notera φ_χ. Et on montre finalement que l'application $\Phi_k : \widehat{G} \to \mathscr{D}_k$ donnée par $\chi \to \varphi_\chi$ a toutes les propriétés requises, en particulier la surjectivité: φ étant un élément quelconque de $\mathscr{D}_k$, il existe un χ tel que $\varphi = \varphi_\chi$, impliquant le théorème d'existence du corps de classes.

Ainsi s'achève le mémoire [6] de 1940, dans lequel Chevalley donne un exposé complet de la théorie du corps de classes dans sa nouvelle formulation extrêmement élégante, avec une démonstration purement arithmétique. C'est bien sûr un de ses travaux les plus importants de Chevalley, et on pourrait dire que cette théorie a enfin trouvé sa formulation définitive. Mais on ne peut pas dire qu'elle a cessé de se développer après ce mémoire.

*

Le développement le plus remarquable, surtout du point de vue méthodologique, serait sans doute vu dans la reconstruction de notre théorie dans le cadre de la théorie cohomologique dans les 1950 dont Chevalley a donné un exposé dans ses leçons à Nagoya [8]. Comme M. Tate voudra bien en parler dans l'article suivant[4] , je me limiterai à ajouter quatre ensembles de remarques avant de terminer mon Introduction.

[4] see ⋆.

(1) Il est naturel que la notion d'idèle introduite par Chevalley et utilisée par lui avec un tel succès ait attiré l'attention des mathématiciens. Artin a eu, en particulier, l'idée de fonder la théorie des fonctions L de Hecke au moyen des idèles. Une de ses élèves, M$^{\text{lle}}$ Matchett, a montré dans un travail en 1946 (qui n'a malheureusement pas été publié) que les fonctions L de Hecke peuvent être en effet définies comme une intégrale de certaines fonctions sur le groupe des idèles. Tate en a donné un exposé dans sa Thèse en 1950 (publiée seulement en 1967 dans [1]), où il a ajouté une découverte importante que les équations fonctionnelles de type bien connu auxquelles satisfont ces fonctions se dérivent de la formule d'inversion de l'intégrale de Fourier et que cette formule appliquée aux corps de fonctions algébriques d'une variable sur les corps finis (voir infra p.74) donne le théorème de Riemann–Roch. D'un autre côté, Iwasawa a eu juste la même idée vers la même époque indépendamment d'Artin et de son école. Il en a rapporté les résultats à Weil, qui lui a répondu pour lui dire que lui-même et Artin avaient eu la même idée un peu auparavant. Iwasawa a remarqué aussi qu'on peut généraliser la définition des idèles dans les corps de nombres algébriques à ceux dans les algèbres de division sur $\boldsymbol{Q}$, et procéder de même manière. Il en a donné un petit rapport dans la section d'algèbre et d'arithmétique du Congrès International des Mathématiciens à Harvard en 1950, dont on trouve un résumé dans les Actes (Iwasawa [1], *cf.* aussi [1a]). Les fonctions zêta (ou L) pour les algèbres sur les corps de nombres algébriques avaient été d'ailleurs définies par Käthe Hey en 1929, dans une thèse à Hambourg [1] qui n'avait pas été publiés et qui avait contenu une petite erreur, corrigée par Zorn [1] qui a remarqué qu'on obtient comme corollaire du résultat corrigé le théorème principal de Hasse [5] d'où découle arithmétiquement la théorie du corps de classes comme Chevalley a montré dans [3] (*cf.* infra p.78). C'est cette méthode qui a été choisie dans Weil [12].

(2) Comme nous l'avons vu plus haut (*cf.* supra p.56), la théorie du corps de classes est valable sur les corps locaux tout aussi bien que sur les corps de nombres algébriques de degrés finis. On s'est aperçu qu'elle est valable aussi sur les corps de fonctions algébriques d'une variable sur les corps finis. Weil [12] utilise le mot *corps-A* ("*A-fields*") comme le terme neutre qui signifie toutes les deux sortes de corps: les corps de nombres algébriques de degré finis et les corps de fonctions algébriques d'une variable sur les corps finis de caractéristiques $p > 0$, c'est-à-dire les corps $\boldsymbol{F}_q(X,Y)$, $q = p^v$, extensions finies de $\boldsymbol{F}_q(X)$. (Pour distinguer les deux, on appelle les premiers les *corps de nombres* et les seconds les *corps de fonctions*.) Comme nous nous sommes occupés jusqu'ici uniquement des premiers, je vais expliquer maintenant de quoi il s'agit en ce qui concerne les seconds.

On se rappelle que Gauss [1] avait déjà considéré les congruences $f(X,Y) \equiv 0 \pmod{p}$ où $f(X,Y) \in \boldsymbol{Z}[X,Y]$ et en avait discuté la résolution de ces congruences en $(X,Y) \in \boldsymbol{Z}^2$. Dedekind [1] avait remarqué qu'il s'agissait là de

l'arithmétique des fonctions algébriques d'une variable sur $\boldsymbol{F}_p$. Dans un grand mémoire [2] en collaboration avec Weber, il avait montré la possibilité de traiter la théorie de fonctions algébriques d'une variables sur $\boldsymbol{C}$ par la même méthode que la théorie des nombres algébriques en utilisant les idéaux, tandis que Hensel et Landsberg [1] avaient développé la même théorie en utilisant les diviseurs au lieu des idéaux. (Cette dernière méthode apparaît plus voisine à la théorie classique de Riemann, les "places" correspondant aux "points" sur la surface de Riemann.) Ces développements ont été faits tout au début de ce siècle.

Dans un travail posthume de Kornblum [1], étudiant à Göttingen, mort jeune à la Première Guerre Mondiale comme un volontaire, on peut s'apercevoir que l'arithmétique du corps de fonctions algébriques d'une variable sur un corps k s'organise plus facilement pour le cas où k est un corps fini que pour le cas où $k = \boldsymbol{C}$ (quoique Kornblum emploie une autre expression.) Kornblum y définit les fonctions L d'après Dirichlet et démontre un analogue du théorème de la progression arithmétique. Mais c'était Artin qui a approfondi cette idée et développé dans sa thèse [1] la théorie des extensions quadratiques de $\boldsymbol{F}_p(X)$ pour lesquelles il a défini la fonction zêta dont il a démontré la validité d'un analogue de l'hypothèse de Riemann pour 14 cas spéciaux. Il a remarqué que cette fonction $\zeta(s)$ se réduit à un polynôme en s, de sorte qu'il est facile d'établir l'équation fonctionnelle pour elle, et la vérification de l'hypothèse de Riemann pour ces cas particuliers se fait par calcul directe. Il a conjecturé bien sûr qu'on pourrait arriver à la même conclusion dans le cas général, ce qui entraînerait en particulier la finitude du nombre des corps quadratiques imaginaires avec une seule classe des idéaux (comme conjecturée depuis Gauss, vérifiée en 1934 par Heilbronn–Linfoot [1]). Je n'entrenai pas dans les détails assez compliquées du développement de cette idée, et mentionnerai tout de suite le résultat capital annoncé par Weil [6] d'avoir démontré vers 1940 cette conjecture pour les corps de fonctions en général (non pas seulement pour les extensions quadratiques de $\boldsymbol{F}_p(X)$ mais pour les extensions finies arbitraires de $\boldsymbol{F}_q(X)$), dont la démonstration complète a été publiée plus tard en [7], [8].

*

On sait que tous les corps finis de caractéristique p sont $\boldsymbol{F}_q$, $q = p^v$, et démontre que toutes les valuations de $\boldsymbol{F}_q(X)$, et donc aussi de $\boldsymbol{F}_q(X,Y)$, extensions algé-briques de $\boldsymbol{F}_q(X)$, sont non-archimédiennes. Soit V l'ensemble de toutes ces valuations. Pour $\alpha \in \boldsymbol{F}_q(X,Y)$, $v \in V$, on a $v(\alpha) = 1$ pour presque toutes les valuations, c'est-à-dire que $v(\alpha) \neq 1$ n'a lieu que pour un nombre fini de $v \in V$, et on peut "normaliser" v de sorte que $\prod_v v(\alpha) = 1$ pour tous les $\alpha \in \boldsymbol{F}_q(X,Y)$, $\alpha \neq 0$. Et dans le cas où k est un corps de nombres algébriques de degré fini, on a vu (p.67 infra) qu'on peut aussi "normaliser" les valuations de sorte qu'il n'y a qu'un nombre fini de v pour lesquels on ait $v(\alpha) \neq 1$ et que

"la formule de produit" $\prod_v v(\alpha) = 1$ soit valable. Ainsi les corps-*A* satisfont à deux axiomes suivants:

A_1 : *Il y a un ensemble V de valuations de k pour lesquelles on a* $v(\alpha) = 1$ *pour presque tous les* $\alpha \in k^\times$, *et* $\prod_v v(\alpha) = 1$ *pour tous les* $\alpha \in k^\times$.

A_2 : *Pour au moins un élément v de V*, (i) *ou* (ii) *a lieu*:

(i) *v est discrète et le corps des résidus est fini*.

(ii) *v est archimédienne, et le corps complet* k_v *est* $\boldsymbol{R}$ *ou* $\boldsymbol{C}$.

Artin et Whaples [1] ont montré que les corps-A sont les seuls corps qui satisfassent aux A_1, A_2. Ainsi ces axiomes caractérisent les corps-A.

Soit donc *k* un corps-A, c'est-à-dire un corps de nombres algébriques de degré fini ou bien un corps de fonctions algébriques d'une variable sur un corps fini,et soit *V* l'ensemble de valuations normalisées de *k* satisfaisant à A_1, A_2. Les éléments α du produit direct $\prod_v k_v$ des corps complétés pour lesquels $v(\alpha) \leq 1$ pour presque tous les $v \in V$ forment évidemment un sous-anneau de $\prod_v k_v$ qui sera noté A_k et appelé l'*anneau du adèles* de *k*. On appellera *adèles* les éléments de A_k. Les *idèles* de *k* ne sont que les éléments inversibles de A_k, dont l'ensemble J_k forme le groupe des idèles de *k* que nous avons déjà rencontré pour le cas où *k* est un corps de nombres algébriques. On constate maintenant que la théorie du corps de classes développée par Chevalley dans son mémoire [6] de 1940 reste valable telle quelle pour l'autre cas de fonctions algébriques (avec quelques petites simplifications) et voici cette théorie pour les corps-A.

(3) On se rappelle que Hensel [1] avait préconisé dès le début de ce siècle une autre méthode que celle de Dedekind pour établir l'arithmétique des corps de nombres algébriques. Nous allons décrire son idée en nous servant des terminologies concernant les valuations d'un corps *k* que nous avons introduites plus haut (infra p.34), en particulier celles archimédiennes et non-archimédiennes, les places de *k* représentant les classes d'équivalence des valuations induisant les mêmes topologies à *k* et la complétion k_v de *k* à chacune de ces places. On commence par remarquer que pour $k = \boldsymbol{Q}$, il n'y a qu'une seule place archimédienne qu'on notera p_∞, à laquelle la complétion $\boldsymbol{Q}_{p_\infty}$ s'identifie avec $\boldsymbol{R}$ et une infinité dénombrable de places non-archimédiennes dont chacune correspond à un nombre premier *p*. On dénotera cette place simplement par *p* et la complétion de $\boldsymbol{Q}$ à *p* par $\boldsymbol{Q}_p$ qu'on appelle le *corps des nombres p-adiques*. On voit que dans tout corps *k* avec une valuation non-archimédienne φ, le sous-ensemble $\{\alpha \in k; \varphi(\alpha) \leq 1\}$ forme un sous-anneau de *k* qu'on appelle l'*anneau de valuation* A_φ pour φ de *k*, et le sous-ensemble $I_\varphi = \{\alpha \in k; \varphi(\alpha) < 1\}$ de A_φ forme l'idéal maximal de A_φ qu'on appelle l'*idéal de valuation* de A_φ (ou de *k*) pour φ. D'ailleurs A_φ et I_φ ne dépendent que de la classe d'équivalence à laquelle appartient φ, donc de la place de φ. Dans le cas où $k = \boldsymbol{Q}$ et la place $= p$, l'anneau A_p (c'est-à-dire A_φ, φ étant une valuation appartenant à la place *p*, la même remarque vaut pour la notation I_p) se compose des nombres rationnels m/n avec $v_p(m) \geq v_p(n)$ où $m, n \in \boldsymbol{Z}$ et $v_p(n)$ pour $n \in \boldsymbol{Z}^\times$ désigne

l'exposant de p dans la décomposition canonique de n. (On pose $v_p(0) = \infty$ où $v_p(0) > v_p(n)$ pour tout $n \in \boldsymbol{Z}^\times$.) De même I_p se compose des nombres rationnels m/n avec $v_p(m) > v_p(n)$. On voit que le corps résiduels $A_p/I_p \cong \boldsymbol{F}_p$ et que l'ensemble des valeurs $\{\varphi(a), a \in \boldsymbol{Q}\}$ n'est autre que $\{c^n, n \in \boldsymbol{Z}\}$ où c est une constante réelle et positive < 1 telle que $\varphi(p) = c$. En posant $w(a) = \log_c \varphi(a)$, on aura $w(a) = v_p(m) - v_p(n) \in \boldsymbol{Z}$ où $a = m/n$ et $v_p(n)$ signifie la fonction que nous avons défini. La fonction $w : \boldsymbol{Q} \to \boldsymbol{Z}$ a évidemment les propriétés $w(ab) = w(a) + w(b); w(a+b) \geq \min(w(a), w(b)); w(p) = 1$. On appellera w la *valuation exponentielle normalisée* de $\boldsymbol{Q}$ à la place p. L'ensemble des valeurs $\{\varphi(a); a \in \boldsymbol{Q}\}$ et celui des valeurs $\{w(a); a \in \boldsymbol{Q}\}$ s'obtiennent par les l'applications bijectives $w(a) = \log_c \varphi(a)$, $\varphi(a) = c^{w(a)}$; ils sont les ensembles discrets de $\boldsymbol{R}$.

En résumé, $\boldsymbol{Q}$ a une infinité dénombrable de places p, pour lesquelles les corps résiduels sont les corps finis $\boldsymbol{F}_p$, et les ensembles des valeurs sont discrets. Et on voit facilement que la valuation (ordinaire ou exponentielle) de $\boldsymbol{Q}$ à la place p se prolonge naturellement et uniquement dans la complétion $\boldsymbol{Q}_p$, et dans celle-ci il n'y a qu'une seule place, prolongée de $\boldsymbol{Q}$, avec les valuations discrètes (toutes équivalentes) au corps résiduel fini. Par extension, on appellera un *corps local* tout corps avec les valuations discrètes avec les corps résiduels finis, toutes équivalentes donnant naissance ainsi à une seule place, et une seule topologie, complet par rapport à la topologie induite. On voit dans $\boldsymbol{Q}_p$ le premier exemple d'un tel corps.

Si l'on suppose connue la théorie des idéaux de Dedekind dans une extension finie k de $\boldsymbol{Q}$, on voit que chaque idéal premier P de k détermine une place, c'est-à-dire une classe d'équivalence de valuations discrètes avec le corps résiduel fini $\boldsymbol{F}_q$ où $q = N_{k/\boldsymbol{Q}}(P)$, et la complétion k_P, qu'on appelle le *corps de nombres P-adiques*, de k à la place P, sera reconnue comme un autre exemple de corps locaux. Le cardinal $q = N_{k/\boldsymbol{Q}}(P)$ de $\boldsymbol{F}_q$ est alors une puissance d'un nombre premier p, et on voit que k_P est une extension finie de $\boldsymbol{Q}_P$, de degré diviseur de $(k : \boldsymbol{Q})$.

En renversant l'ordre d'idées, on peut arriver comme suit à une définition du *diviseur premier* P de p en considérant d'abord les extensions finies de $\boldsymbol{Q}_p$:

Nous allons considérer les extensions finies des corps locaux en général en modifiant la notation pour le moment. Soient donc k un corps local avec la valuation discrète φ, complet par rapport à la topologie induite par φ, avec le corps résiduel fini à q éléments, (q étant une puissance d'un nombre premier p) et K une extension finie de k. On montre alors que la valuation φ de k se prolonge à une valuation Φ de K d'une manière unique, (si $[K : k] = n$ et $\alpha \in K$, on aura $\Phi(\alpha)^n = \varphi(N_{K/k}(\alpha))$, et K avec cette valuation devient un autre corps local : Φ sera discrète et le corps résiduel de K pour Φ sera corps fini à q^f éléments. On verra aussi que f est un diviseur de $n = [K : k]$ et appellera f et $n/f = e$ le *degré relatif* et l'*indice de ramification* de Φ pour K/k, respectivement. K/k est

dit *non-ramifié* si $e = 1$. On montre de plus que toute fermeture algébrique de k contient une et une seule extension non-ramifiée K qui est galoisienne sur k, $G(K/k)$ étant topologiquement engendré par l'automorphisme de Frobenius de K/k.

*

Retournons maintenant à notre notation habituelle : Soient k un corps de nombres algébriques de degré fini, c'est-à-dire une extension finie de $\boldsymbol{Q}$, et φ une valuation non-archimédienne de k. En restreignant φ sur $\boldsymbol{Q}$, on obtient une valuation non-archimédienne de $\boldsymbol{Q}$ appartenant à une place p. En composant k avec $\boldsymbol{Q}_p$ dans un clôture algébrique $\overline{\boldsymbol{Q}_p}$ de $\boldsymbol{Q}_p$ (par rapport à une immersion de k dans $\overline{\boldsymbol{Q}_p}$), on obtient une extension finie de $\boldsymbol{Q}_p$. On a vu que celle-ci est un autre corps local auquel la valuation φ de $\boldsymbol{Q}_p$ se prolonge d'une seule manière. Désignons par Φ cette valuation prolongée. En restreignant Φ sur k, on obtient une valuation, donc une place de k qu'on notera P. La complétion de k à cette place s'identifie avec $k\boldsymbol{Q}_p$; on la notera k_P et l'appellera le *corps de nombres P-adiques* de k. On a pu ainsi définir la place P de k en utilisant la théorie des extensions des corps locaux indépendamment de la théorie de Dedekind. On peut alors définir les diviseurs $M = P_1^{e_1} \cdots P_r^{e_r}$ dans k comme des produits formels des places de k auxquels on peut faire jouer les rôles des idéaux dans k. On voit de plus, par exemple, que si K/k est une extension galoisienne, et $\overline{P}$ est la place de K prolongeant P de k, $K_{\overline{P}}/k_P$ est aussi galoisienne et $G(K_{\overline{P}}/k_P)$ est isomorphe au groupe de décomposition de $\overline{P}$ dans K/k.

On voit ainsi que l'arithmétique des corps de nombres algébriques de degrés finis peut être développée en plongeant ces corps k dans les corps locaux sans prendre le biais de la théorie de Dedekind. Hensel avait préféré cette méthode et on peut interprêter les résultats de Chevalley sur la théorie des corps de classes comme confirmant cette idée.

(4) Nous allons enfin combler les explications que nous avons renvoyées à plus tard (*cf.* supra p.38, p.60).

Dans notre exposé, nous avons vu l'appellation "corps de classes" apparaître pour la première fois dans les conjectures de Hilbert (p.32 supra): k étant un corps de nombres algébriques de degré fini, l'extension K de k s'appelle le corps de classes sur k s'il jouit des propriétés (i) – (iv). En particulier, l'extension K/k est non-ramifiée et abélienne, et on voit de plus qu'elle est maximale parmi les extensions non-ramifiées et abéliennes. On a vu ensuite que le sens de cette appellation s'est élargi depuis Takagi (p.38 supra); maintenant un corps de classes est devenu synonyme d'une extension abélienne. Pour distinguer, on appelle le corps de classes au sens de Hilbert, le *corps de classes de Hilbert* ou le *corps de classes absolu*. Le propriété "(iv) Tout idéal de k transféré dans K devient principal" est caractéristique pour le corps de classes absolu K/k. On appelle cette proposition le *théorème des idéaux principaux*. J'ai mentionné que ce théorème

a été démontré par Furtwängler [2] en 1930, plus de 15 ans plus tard qu'il avait démontré les autres conjectures de Hilbert. En fait, la démonstration dans Furtwängler [2] est basée sur le résultat d'Artin [5] qui permet de traduire au moyen de sa loi de réciprocité le théorème des idéaux principaux en une proposition sur la théorie des groupes méta-abéliens, c'est-à-dire des groupes finis G avec sousgroupes invariants H tels que G/H et H soient tous les deux abéliens. C'est ce théorème sur les groupes méta-abéliens que Furtwängler [2] a démontré par récurrence sur l'ordre des groupes, non sans difficultés. (Je me permets de rappeler que je me suis occupé d'une simplification de cette démonstration [3].)

On peut se demander d'autre part quelle serait une proposition qui corresponderait au théorème des idéaux principaux dans la théorie générale du corps de classes qui concerne aussi les extensions ramifiée. Herbrand s'est posé cette question et l'a résolue dans son mémoire [4]. (Sans le savoir, je me suis posé la même question et ai publié le résultat, essentiellement le même que Herbrand [4], dans [2]. Plus tard, j'en ai donné un exposé plus systématisé, en utilisant les résultats de Hasse [6].) Je n'entrerai pas dans les détails de ces résultats, parce qu'ils ne sont pas en contact direct avec les travaux de Chevalley. Il faut rappeler aussi que Chevalley n'a rien prononcé sur le théorème des idéaux principaux, qui dépasse pour ainsi dire le cadre de la théorie des extensions abéliennes. Je me permetterai d'ajouter cependant qu'on est conduit, en poursuivant la recherche de ce théorème, au difficile problème de la "capitulation des idéaux", c'est-à-dire la poursuite de la manière dont les idéaux transférés dans les extensions deviennent principaux ou "capitulent." Sur ce problème, il y a des exposés ou des résultats assez récents par Iwasawa [4], Miyake [1], Suzuki [1], [2], mais il me semble encore qu'il s'agit d'un champ nouveau.

*

Je retourne enfin au mémoire [3] de Chevalley en collaboration avec Nehrkorn en 1935 qui a donné la première démonstration purement arithmétique de la théorie du corps de classes. Dans le mémoire [4] de Hasse sur la théorie des algèbres sur les corps de nombres algébriques du degré fini k, un invariant $\left(\frac{A}{P}\right)$ pour une algèbre A sur k et une place P de k qui prend des valeurs rationnels a été défini et une belle formule $\sum_P \left(\frac{A}{P}\right) \equiv 0 \pmod 1$ a été démontrée d'où l'on peut déduire la loi d'Artin. Et, chose importante, la démonstation par Hasse de cette formule n'utilise pas l'analyse. Chevalley et Nehrkorn ont montré qu'on peut déduire de là, également sans analyse, le Théorème B de la Thèse de Chevalley (p.53 supra) et par suite toute la théorie du corps de classes. Une autre méthode plus directe de construire cette théorie moyennant la théorie des algèbres a été conçue également par Chevalley et communiquée à Weil qui l'a utilisée dans son exposé dans son livre [12] comme nous l'avons déjà indiqué.

Ce que Chevalley dit dans le dernier passage de l'Introduction de ce mémoire [3] me semble digne d'attention du lecteur. Le mémoire [4] de Chevalley, où se trouve démontrée "l'hypothèse de M. Artin" disant que tout corps finis sont "quasi-algébriquement fermés" est cité dans la bibliographie de [3]. C'est un mémoire de 3 pages seulement, mais qui a été cité peut-être les plus nombreuses fois parmi les travaux de Chevalley et a exercé par conséquent beaucoup d'influence. Chevalley s'est posé la question: si le corps de toutes les racines de l'unité ne serait pas quasi-algébriquement fermé, et ajoute: question reste pour le moment ouverte. Je crois que cette question reste encore ouverte.

J'arrête ici mon exposé en priant M. Tate d'achever la suite[5].

References

E. Artin

[1] Quadratische Körper im Gebiet der höheren Kongruenzen, Math. Z., **19** (1924).

[2] Über eine neue Art von *L*-Reihen, Abh. Hamburg, **1** (1924).

[3] Beweis des allgemeinen Reziprozitätsgesetzes, Abh. Hamburg, **5** (1927).

[4] Über die Bewertungen algebraischer Zahlkörper, J. Reine Angew. Math., **164** (1932).

[5] Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz, Abh. Hamburg, **7** (1929).

[6] Zur Theorie der *L*-Reihen mit allgemeinen Gruppencharakteren, Abh. Hamburg, **8** (1930).

[7] Gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper, J. Reine Angew. Math., **164** (1932).

E. Artin and J. Tate

[1] Class Field Theory, Benjamin, New York, 1967.

E. Artin and G. Whaples

[1] Axiomatic characterization of fields by the product formula for valuations, Bull. Amer. Math. Soc., **51** (1945).

[2] A note on axiomatic characterization of fields, ibid., **52** (1946).

[5] see ⋆.

J. W. S. Cassels and A. ed. Fröhlich

[1] Algebraic Number Theory, Acad. Press, 1967.

C. Chevalley

[1] Sur la structure de la théorie du corps de classes, C. R. Acad. Sci. Paris (1932).

[2] Sur la théorie du corps de classes dans les corps finis et les corps locaux, Thèse à l'Univ. de Paris, publiée dans J. Fac. Sci. Univ. Tokyo, I–2 (1933).

[3] (avec H. Nehrkorn) Sur les démonstrations arithmétiques dans la théorie du corps de classes, Math. Ann., **111** (1935).

[4] Démonstration d'une hypothèse de M. Artin, Abh. Hamburg, **11** (1936).

[5] Généralisation de la théorie du corps de classes pour les extensions infinies, J. Math. Pures Appl., **15** (1936).

[6] La théorie du corps de classes, Ann. Math., **41** (1940).

[7] Deux théorèmes d'arithmétique, J. Math. Soc. Japan, **3** (1951).

[8] Class Field Theory, Lecture Notes, Nagoya Univ., 1953–54.

R. Dedekind

[1] Abriss einer Theorie der höheren Kongruenzen auf einen reellen Primzahl-Modulus, J. Reine Angew. Math., **54** (1857).

[2] (avec Heinrich Weber) Theorie der algebraischen Funktionen einer Veränderlichen, ibid., **92** (1882).

[3] Über die Theorie der Ganzen Algebraischen Zahlen, Supplément XI aux Vorlesungen über Zahlentheorie par Gustav Lejeune Dirichlet, Braunschweig, 1894.

G. L. Dirichlet

[1] Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres, J. Reine Angew. Math., **19** (1839).

[2] Zur Theorie der Komplexen Einheiten, Verh. Preuss. Akad., 1846.

S. Eilenberg and N. Steenrod

[1] Foundations of Algebraic Topology, Princeton Univ. Press, 1952.

G. Eisenstein

[1] Beweis des Reziprozitätsgesetzes für die kubische Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzen komplexen Zahlen, J. Reine Angew. Math., **27** (1844).

[2] Beweis der Allgemeinen Reziprozitätsgesetze Zwischen Reellen und Komplexen Zahlen, Berliner Akad.-Ber., 1850.

G. Frobenius

[1] Die Beziehungen Zwischen den Primidealen eines Algebraischen Körpers und den Substitutionen einer Gruppe, Berlin Akad.-Ber., 1896.

P. Furtwängler

[1] Über die Reziprozitätsgesetze ℓ-ten Potenzresten in algebraischen Zahlkörpern, Math. Ann., **58** (1904); Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörper, ibid., 1907; Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern I–III, ibid., **67** (1909), **72** (1912), **74** (1913).

[2] Beweis des Hauptidealsatzes für Klassenkörper algebraischer Zahlkörper, Hamburg Abh., **7** (1930).

C. F. Gauss

[1] Disquisitiones Arithmeticae, Leipzig, 1801.

[2] Theoria Risiduorum Biquadraticarum II, Comm. Götting. VII, 1832.

J. Hadamard

[1] Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arith-métiques, Bull. Soc. Math. France, **24** (1896).

H. Hasse

[1] Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen, J. Reine Angew. Math., **152** (1923), Über die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen, ibid., **152** (1923).

[2] Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper I, Ia, II, Jber. DMV, **36** (1926), **37** (1927), **40** (1930).

[3] Neue Begründung der komplexen Multiplikation I, II, ibid., **157** (1927), **165** (1931).

[4] Über *p*-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlensysteme, Math. Ann., **104** (1931).

[5] Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper, Math. Ann., **107** (1933).

[6] Normenresttheorie galoischer Zahlkörper mit Anwendungen auf Führer und Diskriminante abelschen Zahlkörper, J. Fac. Sci. Univ. Tokyo Sect., I–2 (1934).

[7] Zur Theorie der abstrakten elliptischen Funktionen I, II, III, J. Reine Angew. Math., **175** (1936).

[8] Vorlesungen über Zahlentheorie, Springer, 1950.

[9] Kurt Hensels entscheidender Anstoss zur Entdeckung des Lokal-Global-Prinzips, J. Reine Angew. Math., **209** (1962).

[10] History of class field theory, In: Algebraic Number Theory, (eds. J. W. S. Cassels and A. Fröhlich), Acad. Press, 1967.

M. Hazewinkel

[1] Local class field theory is easy, Adv. Math., **18** (1975).

E. Hecke

[1] Höhere Modulfunktionen und ihre Anwendung auf die Zahlentheorie, Math. Ann., **71** (1912).

[2] Über die Konstruktion relativ-Abelscher Zahlkörper durch Modulfunktionen von zwei Variablen, Math. Ann., **74** (1913).

[3] Über die *L*-Funktionen und den Dirichletschen Primzahlsatz für einen Beliebigen Zahlkörper, Nachr. Akad. Wiss. Göttingen, 1917.

[4] Theorie der Algebraischen Zahlen, Leipzig 1923, Chelsea 1970.

H. A. Heilbronn

[1] (avec E. H. Linfort) On the imaginary quadratic corpora of class number one, Q. J. Math. Oxford, **5** (1934).

K. Hensel

[1] Theorie der Algebraischen Zahlen, Leipzig, 1908.

K. Hensel and G. Landsberg

[1] Theorie der Algebraischen Funktionen einer Variablen, Leipzig, 1902.

J. Herbrand

[1] Une nouvelle démonstration et généralisation d'un théorème de Minkowski, C. R. Acad. Sci. Paris (1930).

[2] (avec Claude Chevalley) Une nouvelle démonstration du théorème d'existence de la théorie du corps de classes, C. R. Acad. Sci. Paris (1931).

[3] Recherches sur la théorie de la démonstration, Thèse à l'Univ. de Paris, publiée dans Prace Towarzyrtwe Naukowego Warswaskiego, III–33 (1930).

[4] Sur la théorie du genre principal, Hamburg Abh., **9** (1932).

[5] Le devéloppement moderne de la théorie des corps de algebriques: corps de classes et lois de reciprocite, Mém. Sci. Math., **75** (1936).

K. Hey

[1] Analytische Zahlentheorie in Systemen Hyperkomplexer Zahlen, Diss. Hamburg, 1929.

D. Hilbert

[1] Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelschen Zahlkörper, Nachr., Akad. Wiss. Göttingen (1896).

[2] Die Theorie der algebraischen Zahlkörper, Jber. DMV, **6** (1899).

[3] Über die Theorie des relativ-quadratischen Zahlkörper, Math. Ann., **51** (1899).

[4] Über die Theorie der relativ-Abelschen Zahlkörper, Acta Math., **26** (1902).

Y. Ihara

[1] Non-abelian classfields over function fields in special cases, In: Actes Congr. Intern. Math. Nice, 1970.

K. Iwasawa

[1] A note on *L*-functions, In: Proc. Intern. Congress of Math., 1950.

[1a] Letter to J. Dieudonne, In: Zeta Functions in Geometry (Tokyo, 1990), (eds. N. Kurokawa and T. Sunada), Adv. Stud. Pure Math., **21**, Kinokuniya, Tokyo, 1992.

[2] Local Class Field Theory (en japonais), Iwanami, Tokyo, 1980, (trad. russe MNR, Moscow (1983)).

[3] Local Class Field Theory, Oxford Univ. Press, Oxford, 1986.

[4] A note on capitulation problem for number fields, Proc. Japan Acad., **65** (1989).

[5] On papers of Takagi in number theory, In: Teiji Takagi Collected Papers, 2ème éd., Springer, 1990.

S. Iyanaga

[1] Sur un lemme d'arithmétique élémentaire dans la démonstration de la loi générale de réciprocité, C. R. Acad. Sci. Paris (1933).

[2] Über den allgemeinen Hauptidealsatz, Japan J. Math., **7** (1930).

[3] Zum Beweis des Hauptidealsatzes, Hamburg Abh., **10** (1934).

[4] Zur Theorie der Geschlechtermoduln, J. Reine Angew. Math., **17** (1934).

[5] Class Field Theory, Lecture Note, Chicago Univ., 1961.

[6] (Ed.) The Theory of Numbers, North-Holland, 1975.

H. Kornblum

[1] Über die Primfunktionen in einer arithmetischen Progression, Math. Z., **5** (1919).

L. Kronecker

[1] Über Abelsche Gleichungen, Sitzungsber. Preuss. Akad. Wiss., 1877.

[2] Grundzüge einer arithmetischen Theorie der algebraischen Grössen, J. Reine Angew. Math., **92** (1882).

W. Krull

[1] Galoische Theorie der unendlichen algebraischen Erweiterungen, Math. Ann., **100** (1928).

E. Kummer

[1] Über die Zerlegung der aus Wurzeln der Einheit gebildeten komplexen Zahlen in ihre Primfaktoren, J. Reine Angew. Math., **35** (1847).

S. Lang

[1] Algebraic Numbers, Addison Wesley, Reading, Mass., 1963.

[2] Algebraic Number Theory, Addison Wesley, Reading, Mass., 1970.

K. Miyake

[1] Algebraic investigations of Hilbert's theorem 94, Expo. Math., **7** (1989).

A. Ostrowski

[1] Über einige Lösungen der Funktionalgleichung $\varphi(x)\varphi(y) = \varphi(xy)$, Acta Math., **4** (1918).

L. S. Pontrjagin

[1] Topological Groups (en russe), Moscow, 1954 (trad. anglaise, Princeton (1960))

B. Riemann

[1] Über die Anzahl der Primzahlen unter einer gegebenen Grösse, Monatsber. d. Königl. Preuss. Akad. (1859).

P. Samuel

[1] Théorie Algébrique des Nombres, Hermann, 1967.

F. K. Schmidt

[1] Zur Klassenkörper im Kleinen, J. Reine Angew. Math., **162** (1930).

O. Schreier

[1] Über eine Arbeit von Herrn Tschebotareff, Hamburg Abh., **4** (1926).

J.-P. Serre

[1] Corps Locaux, Hermann, 1962.

[2] Complex multiplication, In: Algebraic Number Theory, (eds. J. W. S. Cassels and A. Fröhlich), Acad. Press, 1967.

G. Shimura

[1] On complex multiplications, In: Proc. Intern. Symp. on Alg. Number Theory, Tokyo-Nikko, 1956.

[2] Construction of class fields and zeta-functions of algebraic curves, Ann. of Math., **85** (1967).

[3] Introduction to Arithmetic Theory of Automorphic Functions, Publ. Math. Soc. Japan, Iwanami–Princeton Univ. Press, 1971.

G. Shimura and Y. Taniyama

[1] Complex multiplication of Abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, 1961.

H. Suzuki

[1] A generalization of Hilbert's theorem 94, Nagoya Math. J., **121** (1991).

[2] On the capitulation problem, In: Class Field Theory— Its Centenary and Prospect, (ed. K. Miyake), Adv. St. Pure Math., **30**, Math. Soc. of Japan, 2001.

T. Takagi

[1] Über die im Bereiche der rationalen komplexen Zahlen Abelschen Zahlkörper, J. Coll. Sci. Tokyo, **19** (1903).

[2] Zur Theorie der relativ-Abelschen Zahlkörper I, II, Proc. Phys.-Math. Soc. Japan, II 8 (1915).

[3] Über eine Theorie des relativ-Abelschen Zahlkörpers, J. Coll. Sci. Tokyo, **41** (1920).

[4] Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper, ibid., **44** (1922).

[5] Sur quelques théories généraux de la théorie des nombres algebrique, In: Comptes Rendues Congr. Intern. des Math. Strasbourg, 1920.

[6] Comptes rendu du mémoire d'E. Artin: Beweis des allgemeinen Reziprozitätsgesetzes (en japonais), Bull. Phys. Math. Soc. Japan, **1** (1927).

[7] Théorie Algébrique des Nombres (en japonais), Iwanami, 1948.

Y. Taniyama

[1] Jacobian varieties and number fields, In: Proc. Intern. Symp. on Alg. Number Theory, Tokyo-Nikko, 1956.

J. Tate

[1] Fourier analysis in number fields and Hecke's zeta functions, Thesis, Princeton Univ. (1950), In: Algebraic Number Theory (eds. J. W. S. Cassels and A. Fröhlich), Acad. Press (1967).

N. Tschebotareff

[1] Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, Math. Ann., **95** (1926).

C. De la Vallée-Poussin

[1] Recherches analytiques sur la théorie des nombres premiers, Ann. Soc. sc. Bruxelles, **20** (1896).

H. Weber

[1] Theorie der Abelschen Zahlkörper I, II, Acta Math., **8** (1886), **9** (1887).

[2] Über Zahlengruppen in algebraischen Körpern I, II, III, Math. Ann., **48** (1897), **49** (1897), **50** (1898).

[3] Lehrbuch der Algebra I, II, III, Vieweg, I, 1894; II, 1896; III, 1908.

[4] Zur Theorie der zyklischen Zahlkörper I, II, Math. Ann., **67** (1909), **70** (1911).

A. Weil

[1] L'arithmétique sur une courbe algébrique, C. R. Acad. Sci. Paris (1927).

[2] L'arithmétique sur les courbes algébriques, Acta Math., **52** (1928).

[3] (avec Claude Chevalley) Un théorème d'arithmétique sur les courbes algébriques, C. R. Acad. Sci. Paris (1932).

[4] (avec Claude Chevalley) Über das Verhalten der Integrale erster Gattung bei Automorphismen des Funktionenkörpers, Hamburg Abh., **10** (1934).

[5] Remarques sur les résultats récents de Chevalley, C. R. Acad. Sci. Paris (1936).

[6] On the Riemann hypothesis in function fields, Proc. Natl. Acad. Sci., **27** (1941).

[7] Foundations of algebraic geometry, Amer. Math. Soc. Colloq. Publ., 1946, 2ème éd., 1962.

[8] (a) Sur les Courbes Algébriques et les Variétés Qui s'en Déduisent, (b) Variétés Abéliennes et Courbes Algébriques, Hermann, 1948, 2ème éd., 1971.

[9] Number theory and algebraic geometry, In: Proc. Intern. Congr. Math., Cambridge, 1950.

[10] Sur la théorie du corps de classes, J. Math. Soc. Japan, **3** (1951).

[11] On the theory of complex multiplication, In: Proc. Intern. Symp. on Alg. Number Theory, 1956.

[12] Basic Number Theory, Springer, 1967.

M. Zorn

[1] Note on analytischen hyperkomplexen Zahlentheorie, Abh. Hamburg, **9** (1933).